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

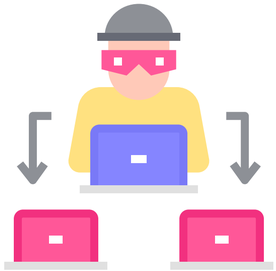
Anh V. Vu, Ben Collier, Daniel R. Thomas, John Kristoff, Richard Clayton, Alice Hutchings

anh.vu@cst.cam.ac.uk

The 34th USENIX Security Symposium, 13–15 August 2025, Seattle, Washington State, USA

DDoS attacks and DDoS-for-hire services

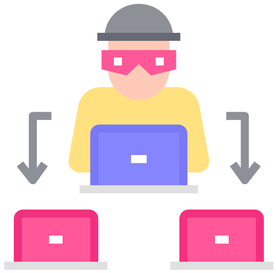
UNIVERSITY OF CAMBRIDGE



thousands of
compromised machine

DDoS attacks and DDoS-for-hire services

UNIVERSITY OF CAMBRIDGE

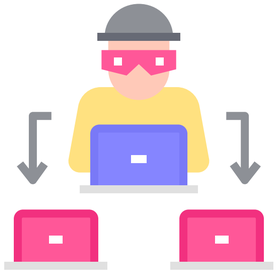


thousands of
compromised machine

targeted machine

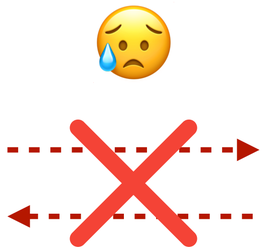
DDoS attacks and DDoS-for-hire services

UNIVERSITY OF CAMBRIDGE



thousands of
compromised machine

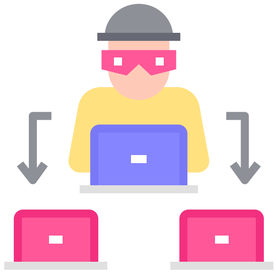
targeted machine



legitimate users

DDoS attacks and DDoS-for-hire services

UNIVERSITY OF CAMBRIDGE

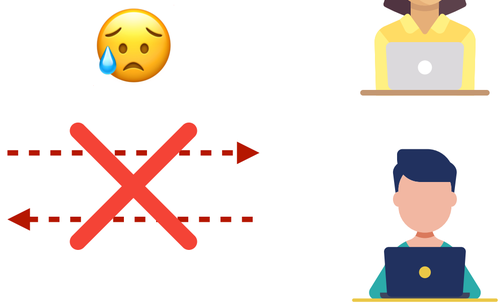


thousands of
compromised machine

But… you don't have to be that bad guy 🧐

- You do not need to have technical skills.
- You have some dollars, for example, $10–20.
- You go online to find DDoS-for-hire services (or booters).
- You make the payment, often in cryptocurrencies.
- You click the ‘attack’ button. Your target is hit!

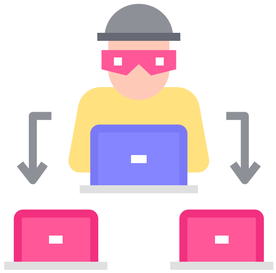
targeted machine



legitimate users

DDoS attacks and DDoS-for-hire services

UNIVERSITY OF CAMBRIDGE

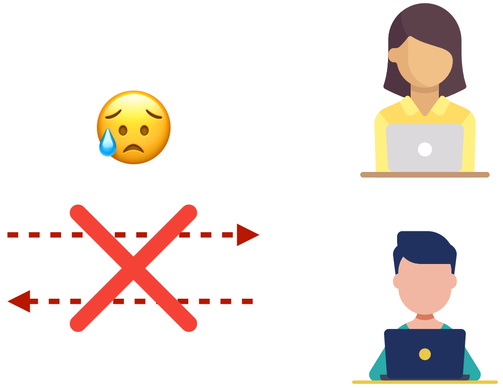


thousands of compromised machine

But… you don't have to be that bad guy 🧐

- You do not need to have technical skills.
- You have some dollars, for example, $10–20.
- You go online to find DDoS-for-hire services (or booters).
- You make the payment, often in cryptocurrencies.
- You click the 'attack' button. Your target is hit!

targeted machine



legitimate users

operating and using booters are illegal in most jurisdictions!

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

6452	5161285	81	54175
Today Attacks	Total Attacks	Running Attacks	Total Users

News

01:47 — Innovations

All layer 7 methods have been updated. "HTTP-CUSTOM" and "HTTP-STORM" methods have been removed because they no longer work. Instead we have added a new method “HTTP-COOKIE” The information about the newly added methods has been updated again today, we recommend you to read the “Methods Info” section before using it or if you do not know how to use it. We are working on adding more new methods and improving the quality of our proxy network.

September 13th

23:32 — Outage

Hello dear users, the problem has been fixed. Now the system is working stably, +5 days have been added to all our active customers due to the problem experienced. Thank you for your understanding.

August 23rd

06:51 — Layer 7 Optimizated

Hello, optimization issue in Layer 7 methods has been fixed. We also added 2 new methods HTTP-SMART and HTTP-QUERY, don't forget to try these methods, they are very effective for Cloudflare!

May 13th

Free Plan

Balance

$0

Concurrents	1
Max Boot Time	60
Premium	✕
API Access	✕
Expire	Never

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

6452	5161285	81	54175
Today Attacks	Total Attacks	Running Attacks	Total Users

News

01:47 **Innovations**

All layer 7 methods have been updated. "HTTP-CUSTOM" and "HTTP-STORM" methods have been removed because they no longer work. Instead we have added a new method “HTTP-COOKIE” The information about the newly added methods has been updated again today, we recommend you to read the “Methods Info” section before using it or if you do not know how to use it. We are working on adding more new methods and improving the quality of our proxy network.

September 13th

23:32 **Outage**

Hello dear users, the problem has been fixed. Now the system is working stably, +5 days have been added to all our active customers due to the problem experienced. Thank you for your understanding.

August 23rd

06:51 **Layer 7 Optimizated**

Hello, optimization issue in Layer 7 methods has been fixed. We also added 2 new methods HTTP-SMART and HTTP-QUERY, don't forget to try these methods, they are very effective for Cloudflare!

May 13th

Free Plan

Balance

$0

Concurrents	1
Max Boot Time	60
Premium	✕
API Access	✕
Expire	Never

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

6452	5161285	81	54175
Today Attacks	Total Attacks	Running Attacks	Total Users

News

01:47 **Innovations**

All layer 7 methods have been updated. "HTTP-CUSTOM" and "HTTP-STORM" methods have been removed because they no longer work. Instead we have added a new method “HTTP-COOKIE” The information about the newly added methods has been updated again today, we recommend you to read the “Methods Info” section before using it or if you do not know how to use it. We are working on adding more new methods and improving the quality of our proxy network.

September 13th

23:32 **Outage**

Hello dear users, the problem has been fixed. Now the system is working stably, +5 days have been added to all our active customers due to the problem experienced. Thank you for your understanding.

August 23rd

06:51 **Layer 7 Optimizated**

Hello, optimization issue in Layer 7 methods has been fixed. We also added 2 new methods HTTP-SMART and HTTP-QUERY, don't forget to try these methods, they are very effective for Cloudflare!

May 13th

Free Plan

Balance

$0

Concurrents	1
Max Boot Time	60
Premium	✕
API Access	✕
Expire	Never

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

Plan Builder

$20 /month

Concurrents: 1

Max Boot Time: 300

Period (months): 1

Premium Access: No

API Access: No

Buy Now

Professional

$115 /month

Concurrents	5
Max Boot Time	1200
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

High-Level

$265 /month

Concurrents	15
Max Boot Time	1800
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Expert

$500 /month

Concurrents	30
Max Boot Time	3600
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Business

$1000 /month

Concurrents	60
Max Boot Time	7200
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Boss

$2000 /month

Concurrents	100
Max Boot Time	14400
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

Plan Builder

$20 /month

Concurrents: 1

Max Boot Time: 300

Period (months): 1

Premium Access: No

API Access: No

Buy Now

Professional

$115 /month

Concurrents	5
Max Boot Time	1200
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

High-Level

$265 /month

Concurrents	15
Max Boot Time	1800
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Expert

$500 /month

Concurrents	30
Max Boot Time	3600
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Business

$1000 /month

Concurrents	60
Max Boot Time	7200
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Boss

$2000 /month

Concurrents	100
Max Boot Time	14400
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

Plan Builder

$20 /month

Concurrents: 1

Max Boot Time: 300

Period (months): 1

Premium Access: No

API Access: No

Buy Now

Professional

$115 /month

Concurrents	5
Max Boot Time	1200
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

High-Level

$265 /month

Concurrents	15
Max Boot Time	1800
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Expert

$500 /month

Concurrents	30
Max Boot Time	3600
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Business

$1000 /month

Concurrents	60
Max Boot Time	7200
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

Boss

$2000 /month

Concurrents	100
Max Boot Time	14400
Period	1 month
Premium	✓
API Access	✓
Prioritized support	✓
Unlimited Attacks	✓

Buy Now

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

Stress Panel

Layer 3/4 | Layer 7

URL * | Time *

https://target.com | 60

Request per IP * | Request Method *

1-64 | GET

Method *

HTTP-CONNECT

Concurrents

5

Send Attack

Attacks

Stop All Attacks | Schedule

ID	Target	Method	Expire	Action
No running attacks				

10

MAIN

- Dashboard

PANEL

- Stress Hub
- Purchase
- Support
- Deposit
- Purchase Add-on
- API Manager
- Methods Info
- FAQ

CONTACT

- Telegram

Stress Panel

Layer 3/4 | Layer 7

URL *

https://target.com

Time *

60

Request per IP *

1-64

Request Method *

GET

Method *

HTTP-CONNECT

Concurrents

5

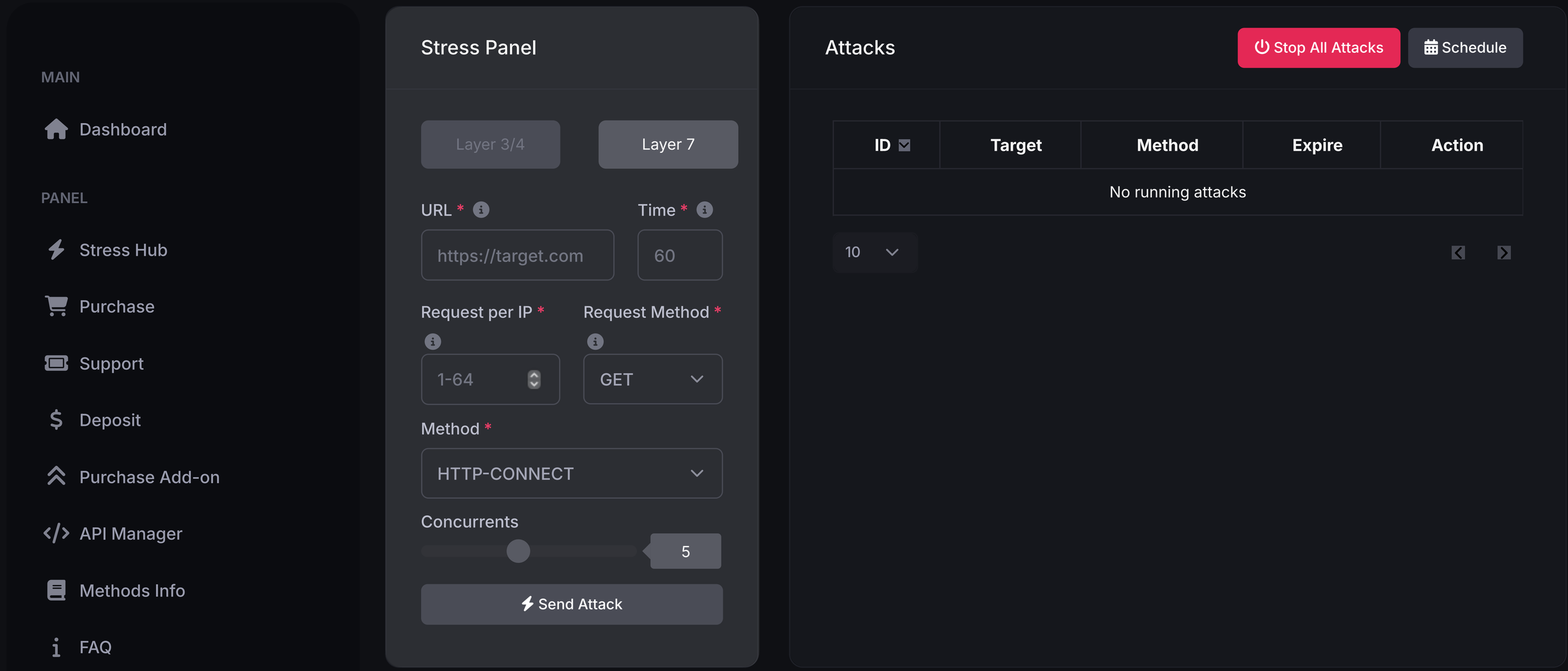
Send Attack

Attacks

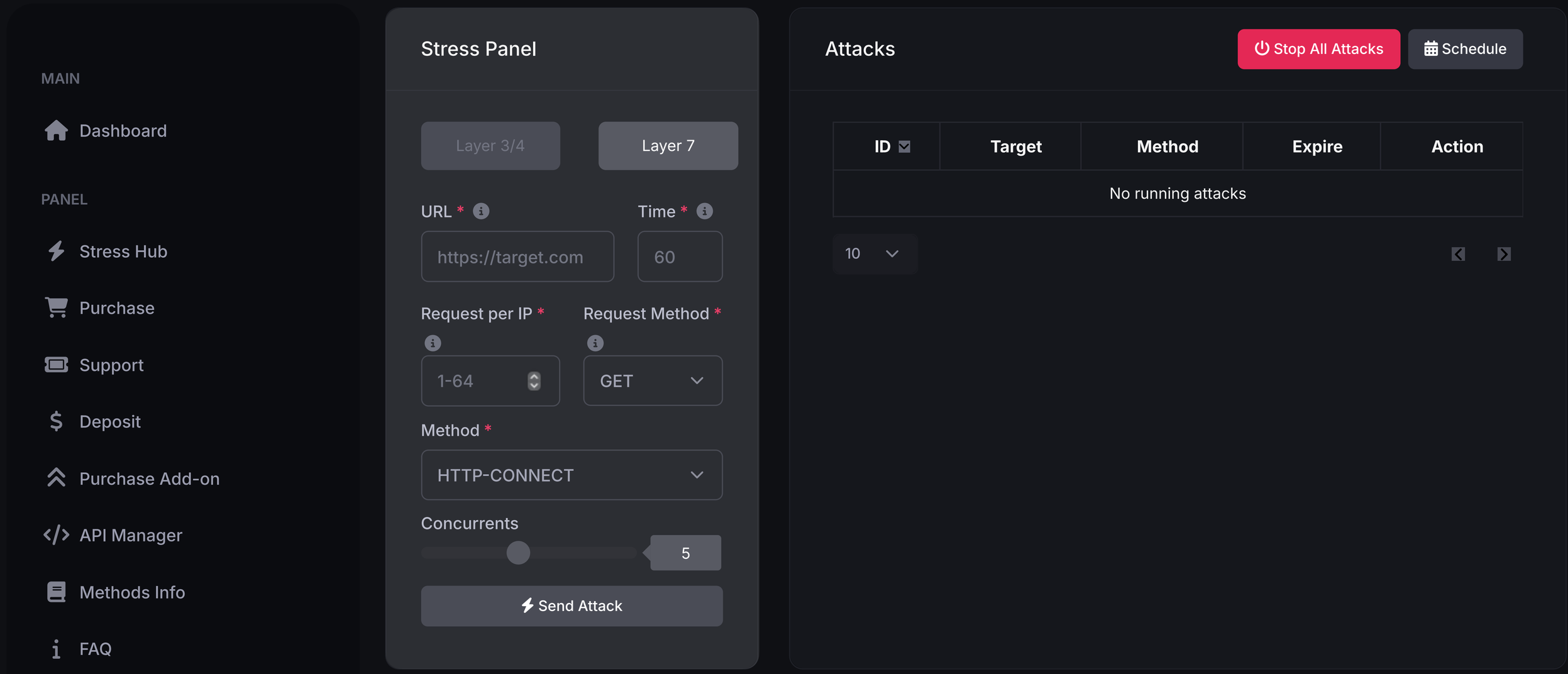
Stop All Attacks | Schedule

ID	Target	Method	Expire	Action
No running attacks				

10



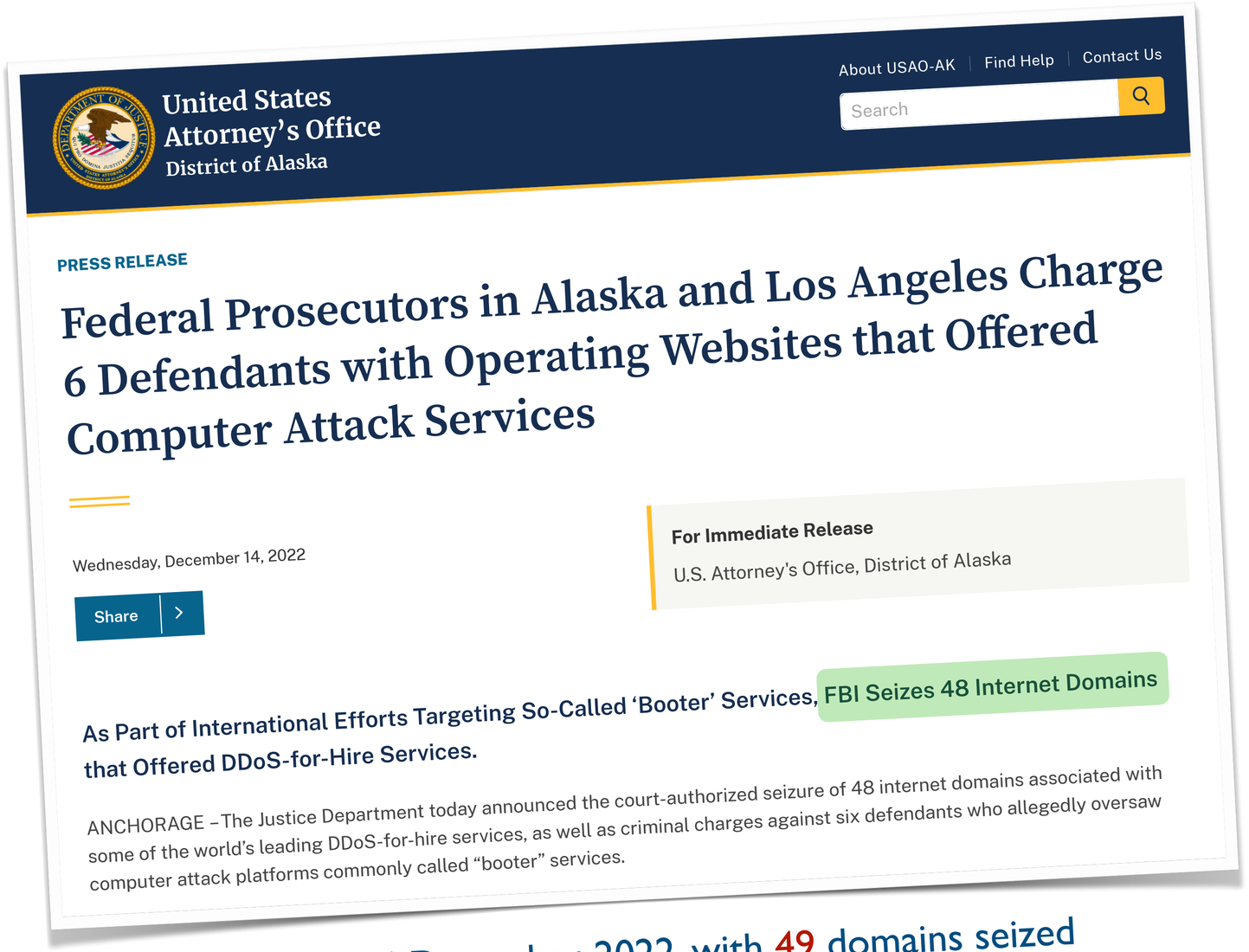
- No technical skills required. The free trial plans work!
- The attack period is often short, but multiple sessions can be combined.



- No technical skills required. The free trial plans work!
- The attack period is often short, but multiple sessions can be combined.
- Facilitates high-volume but low-value cybercrimes that can evade police attention.

The ongoing global takedowns against booters…

UNIVERSITY OF CAMBRIDGE



United States Attorney's Office
District of Alaska

About USAO-AK | Find Help | Contact Us

Search

PRESS RELEASE

Federal Prosecutors in Alaska and Los Angeles Charge 6 Defendants with Operating Websites that Offered Computer Attack Services

Wednesday, December 14, 2022

Share

For Immediate Release

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

As Part of International Efforts Targeting So-Called 'Booter' Services, FBI Seizes 48 Internet Domains that Offered DDoS-for-Hire Services.

ANCHORAGE – The Justice Department today announced the court-authorized seizure of 48 internet domains associated with some of the world's leading DDoS-for-hire services, as well as criminal charges against six defendants who allegedly oversaw computer attack platforms commonly called "booter" services.

First wave, 14 December 2022, with 49 domains seized

The ongoing global takedowns against booters…

UNIVERSITY OF CAMBRIDGE

United States Attorney's Office
District of Alaska

PRESS RELEASE

Federal Prosecutors in Alaska and
6 Defendants with Operating Webs
Computer Attack Services

Wednesday, December 14, 2022

Share

For Imme
U.S. Attor

As Part of International Efforts Targeting So-Called 'Booter' Se
that Offered DDoS-for-Hire Services.

ANCHORAGE – The Justice Department today announced the court-authorize
some of the world's leading DDoS-for-hire services, as well as criminal charg
computer attack platforms commonly called "booter" services.

United States Attorney's Office
Central District of California

About CDCA | Find Help | Contact Us

Search

PRESS RELEASE

Federal Authorities Seize 13 Internet Domains
Associated with 'Booter' Websites that Offered DDoS
Computer Attack Services

Monday, May 8, 2023

Share

For Immediate Release

U.S. Attorney's Office, Central District of California

Four Men Affiliated with Now-Defunct Booter Services Have Pleaded Guilty

LOS ANGELES – As part of an ongoing initiative targeting computer attack "booter" services, the Justice Department today announced the court-authorized seizure of 13 internet domains associated with these DDoS-for-hire services.

First wave, 14 December 2022, with 49 domains seized

Second wave, 5 May 2023, with
13 more domains seized

THIS WEBSITE HAS BEEN SEIZED

The FBI has seized this website for operating as a DDoS-for-hire service. This action has been taken in conjunction with Operation PowerOFF, a coordinated international law enforcement effort to dismantle criminal DDoS-for-hire services worldwide. **DDoS attacks are illegal.**

Law enforcement agencies have seized databases and other information relating to these services. **Anyone operating or utilizing a DDoS service is subject to investigation, prosecution, and other law enforcement action.**

For more information, please visit:

https://www.fbi.gov/contact-us/field-offices/anchorage/fbi-intensify-efforts-to-combat-illegal-ddos-attacks

Multiple datasets from both academics and industry

UNIVERSITY OF CAMBRIDGE

- 20.7M+ ground-truth traffic records from splash pages
- Discussion on booters' Telegram channels, 34k+ messages
- Web traffic to 94 seized and resurrected domains, by Similarweb

Multiple datasets from both academics and industry

UNIVERSITY OF CAMBRIDGE

- 20.7M+ ground-truth traffic records from splash pages
- Discussion on booters' Telegram channels, 34k+ messages
- Web traffic to 94 seized and resurrected domains, by Similarweb
- Global DDoS attack records
  - UDP Amplification DDoS attacks from honeypot
    - Hopscotch, 4.6M+ records [1]
    - AmpPot, 9.8M+ records [2]

[1] Daniel R. Thomas, Richard Clayton, and Alastair R. Beresford. 1000 Days of UDP Amplification DDoS Attacks. Proceedings of the APWG Symposium on Electronic Crime Research (eCrime), 2017.

[2] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. AmpPot: Monitoring and Defending against Amplification DDoS Attacks. Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2015.

Multiple datasets from both academics and industry

UNIVERSITY OF CAMBRIDGE

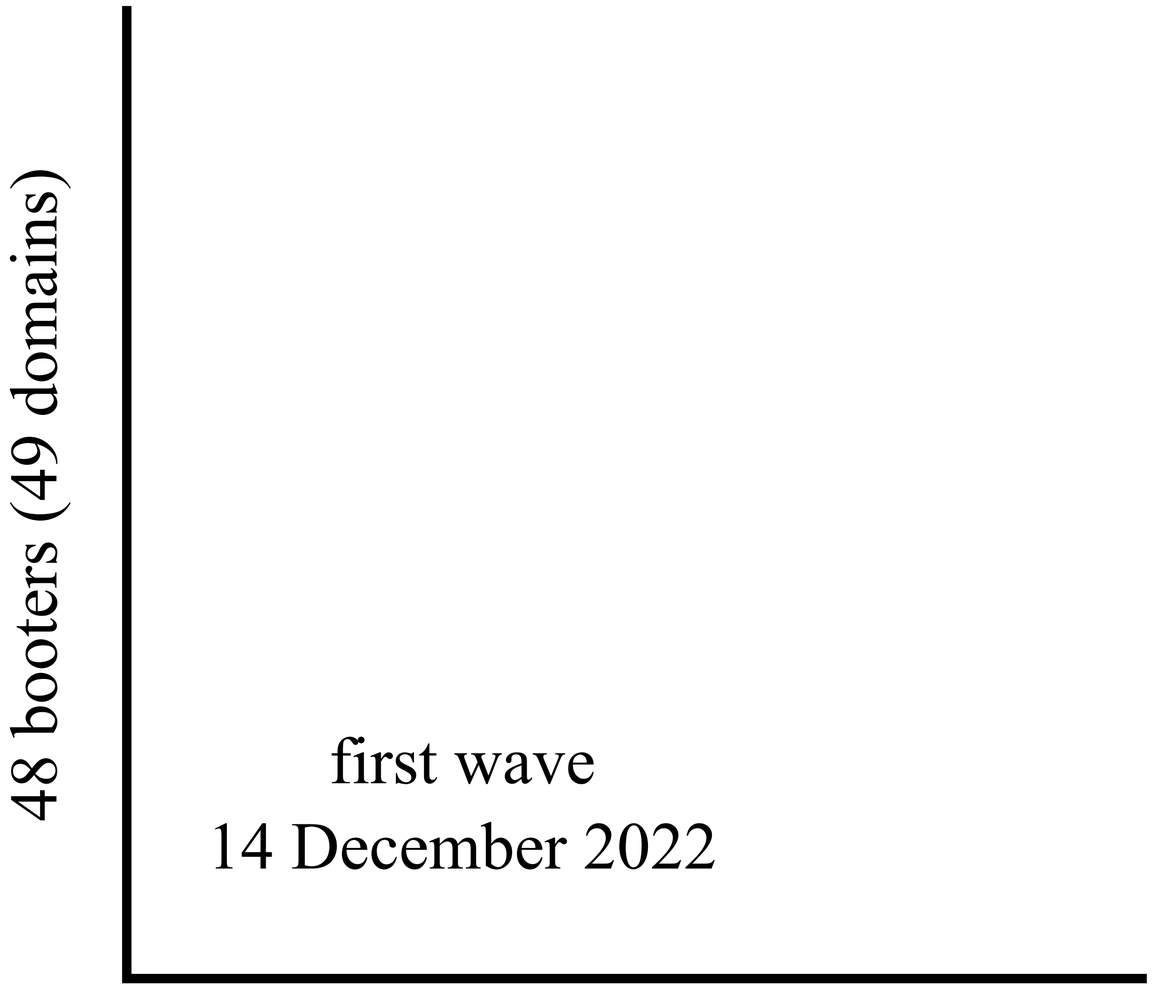
- 20.7M+ ground-truth traffic records from splash pages
- Discussion on booters' Telegram channels, 34k+ messages
- Web traffic to 94 seized and resurrected domains, by Similarweb
- Global DDoS attack records
  - UDP Amplification DDoS attacks from honeypot
    - Hopscotch, 4.6M+ records [1]
    - AmpPot, 9.8M+ records [2]
  - 32.9M+ DDoS attack records (both TCP-based and UDP-based) from NETSCOUT
  - Self-reported attack statistics, 207 booters over two years

[1] Daniel R. Thomas, Richard Clayton, and Alastair R. Beresford. 1000 Days of UDP Amplification DDoS Attacks. Proceedings of the APWG Symposium on Electronic Crime Research (eCrime), 2017.

[2] Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow. AmpPot: Monitoring and Defending against Amplification DDoS Attacks. Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), 2015.

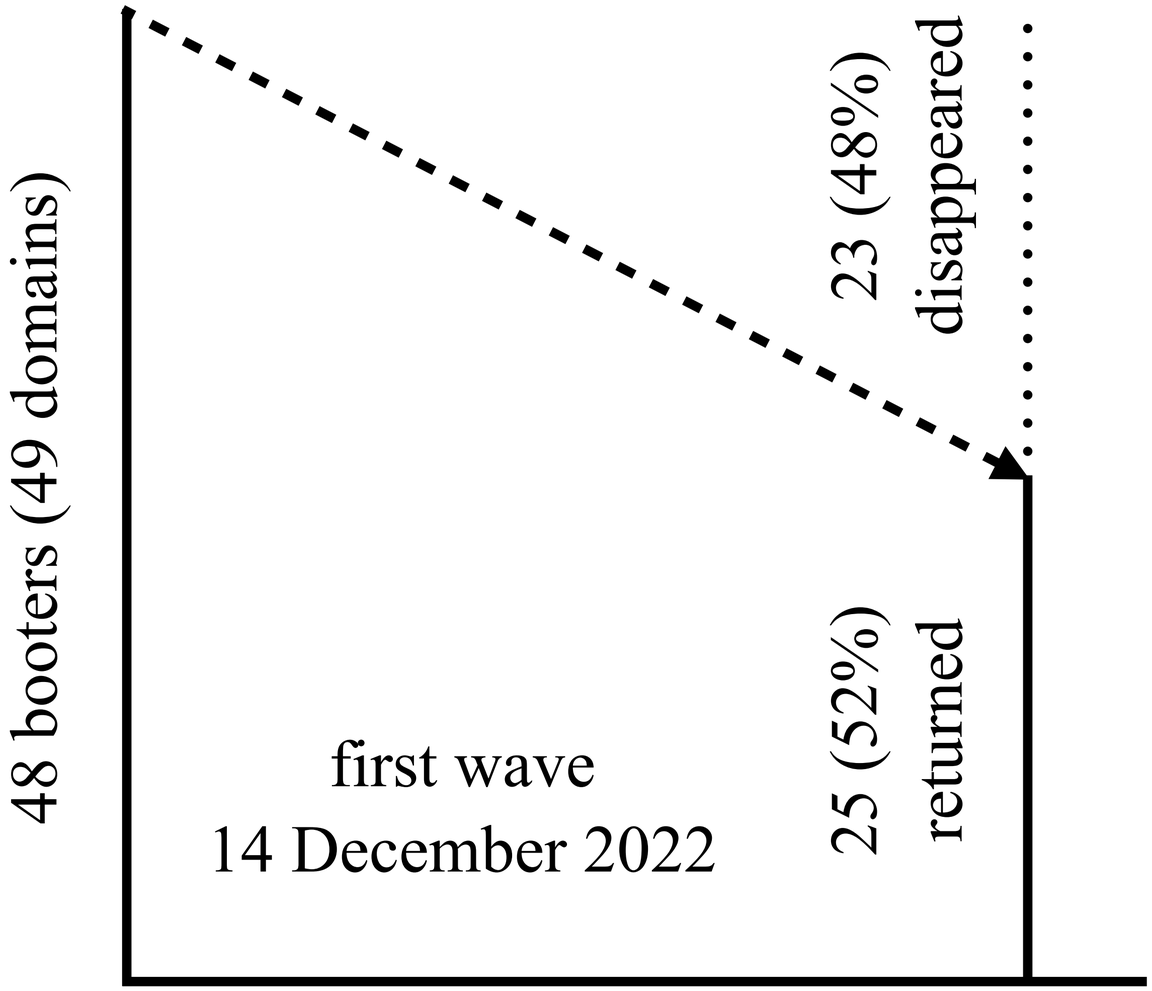
Booter resurrections were fast!

UNIVERSITY OF CAMBRIDGE



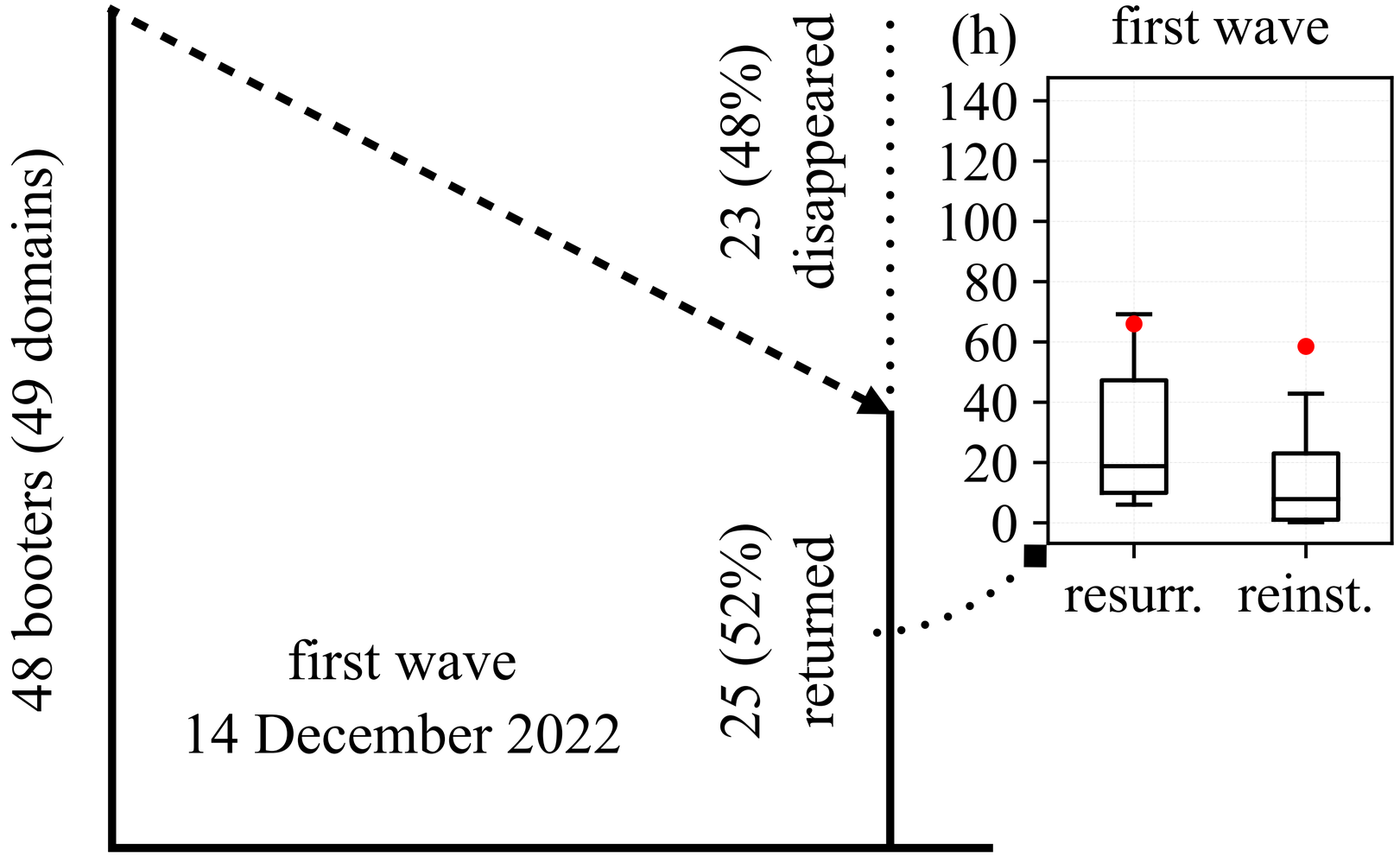
Booter resurrections were fast!

UNIVERSITY OF CAMBRIDGE



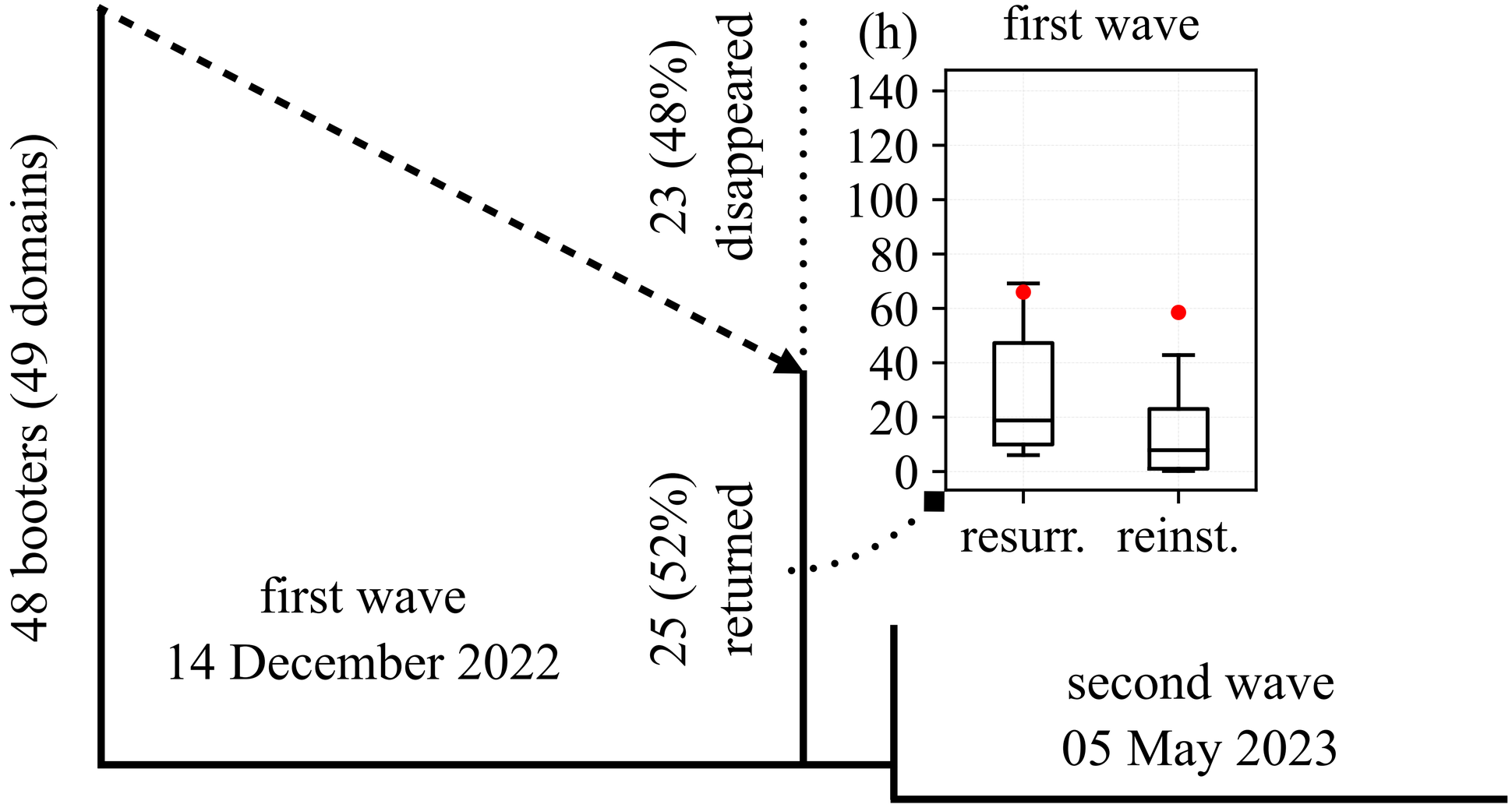
Booter resurrections were fast!

UNIVERSITY OF CAMBRIDGE



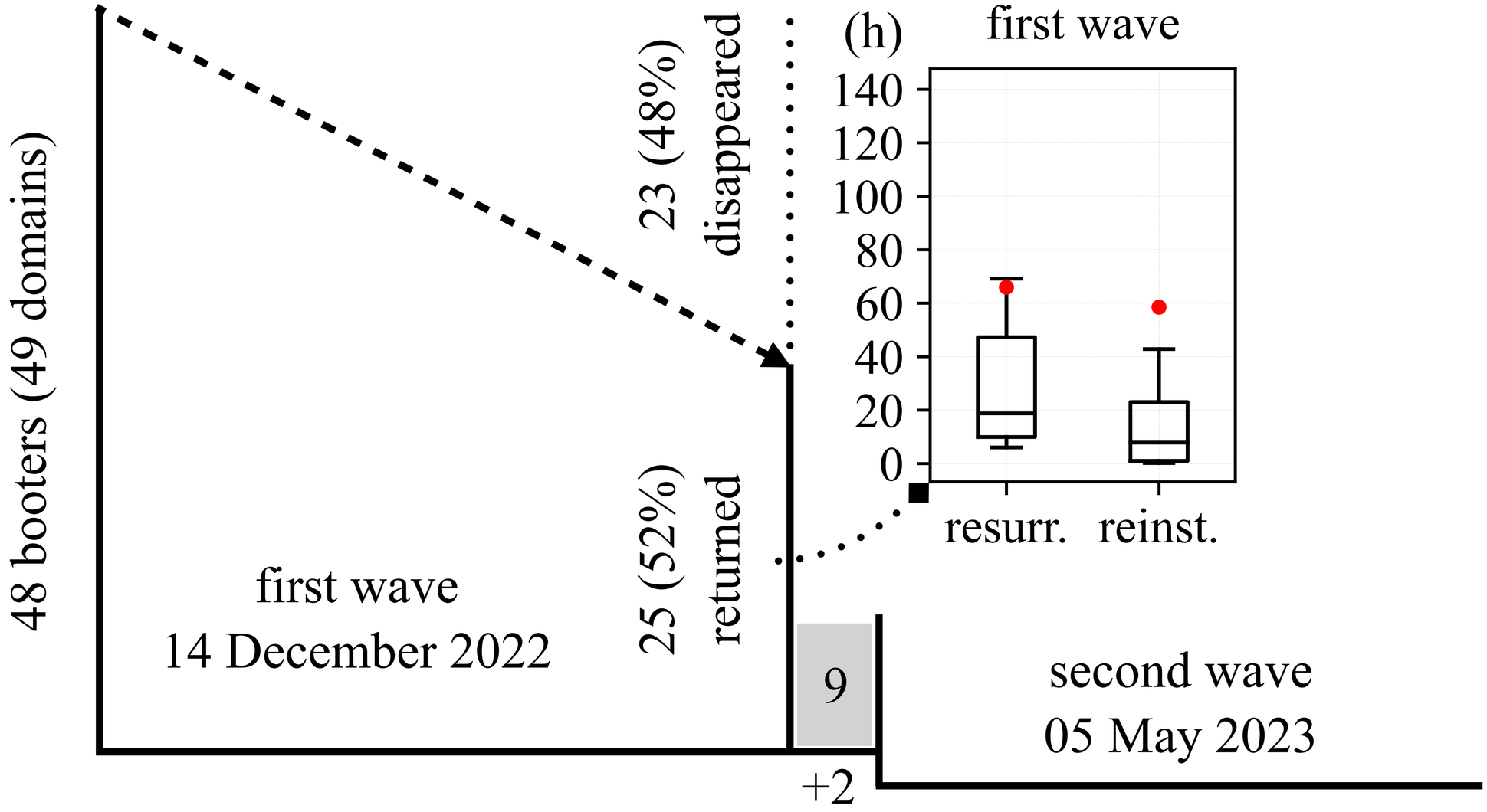
Booter resurrections were fast!

UNIVERSITY OF CAMBRIDGE



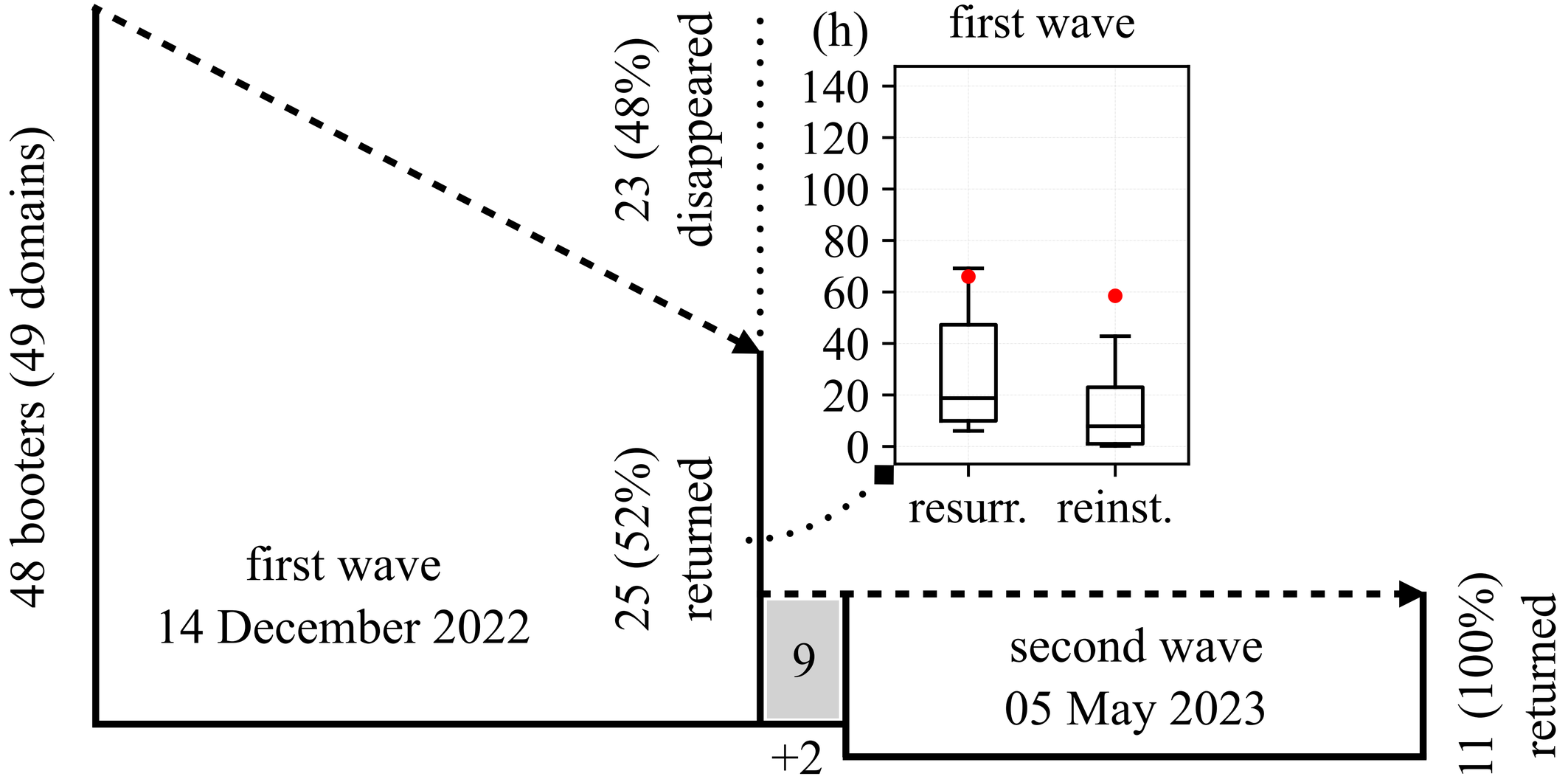
Booter resurrections were fast!

UNIVERSITY OF CAMBRIDGE



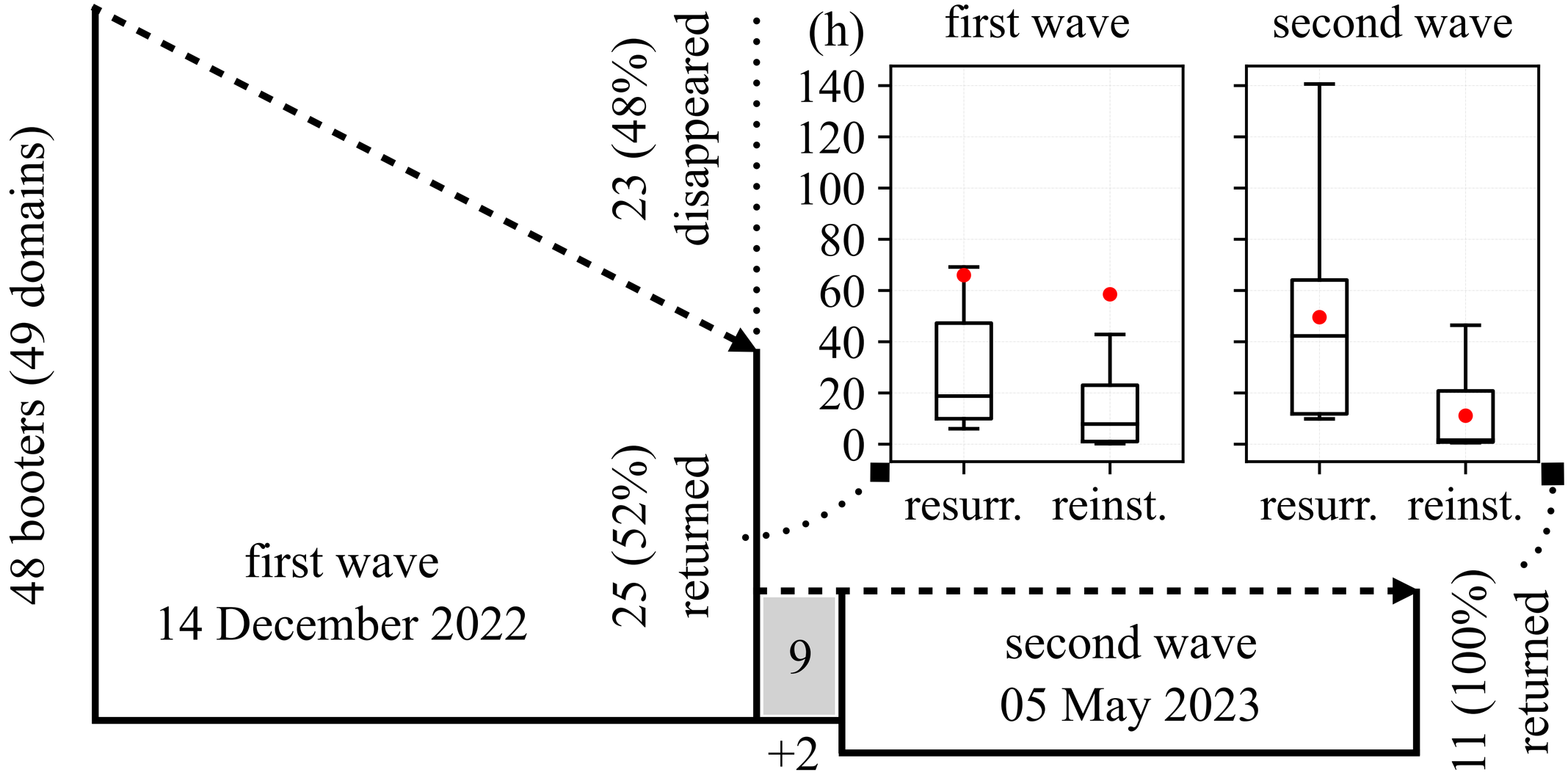
Booter resurrections were fast!

UNIVERSITY OF CAMBRIDGE



Booter resurrections were fast!

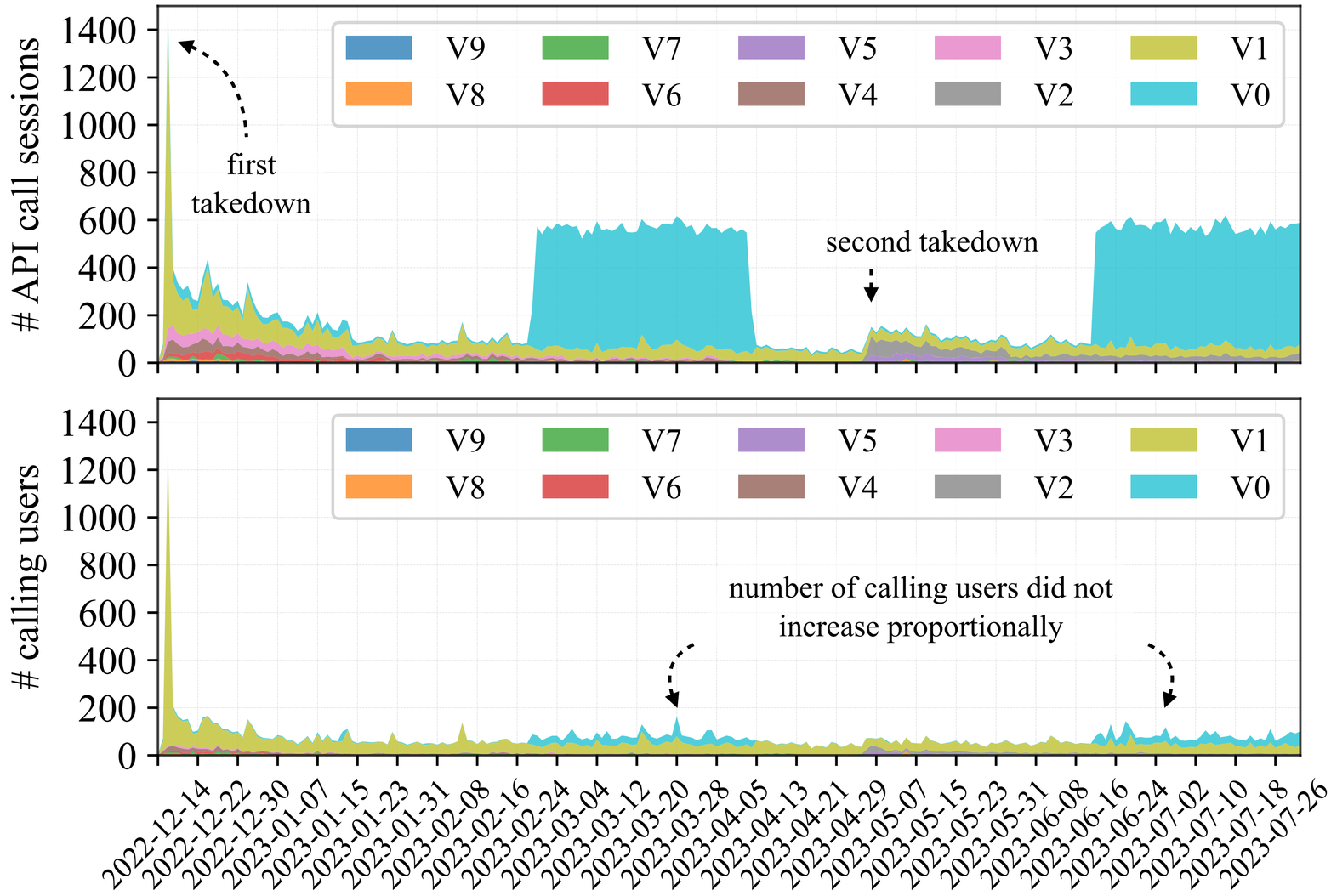
UNIVERSITY OF CAMBRIDGE



Ground-truth traffic — API calls

UNIVERSITY OF CAMBRIDGE

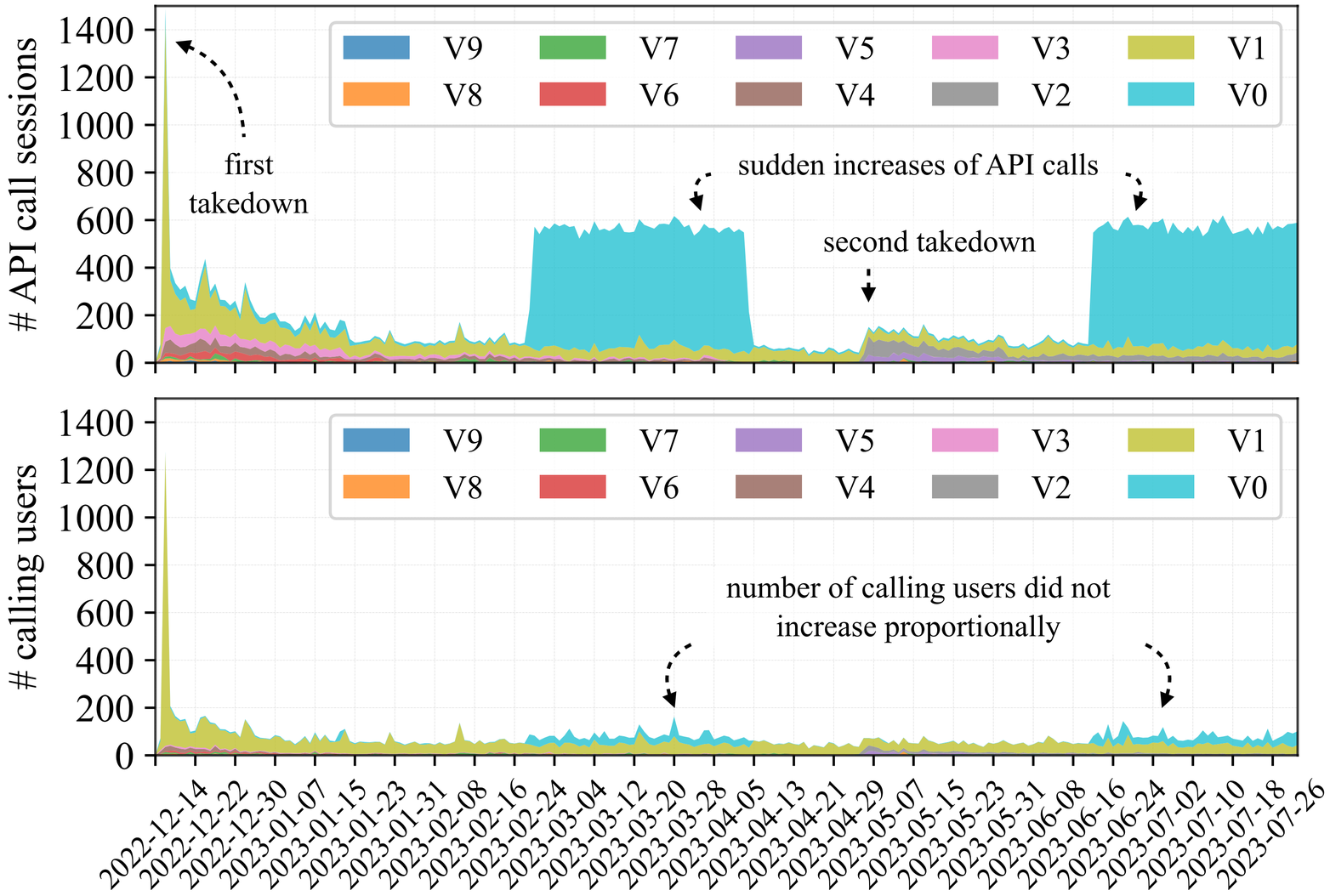
- Major booters provide APIs to others to create second-tier booters.



Ground-truth traffic — API calls

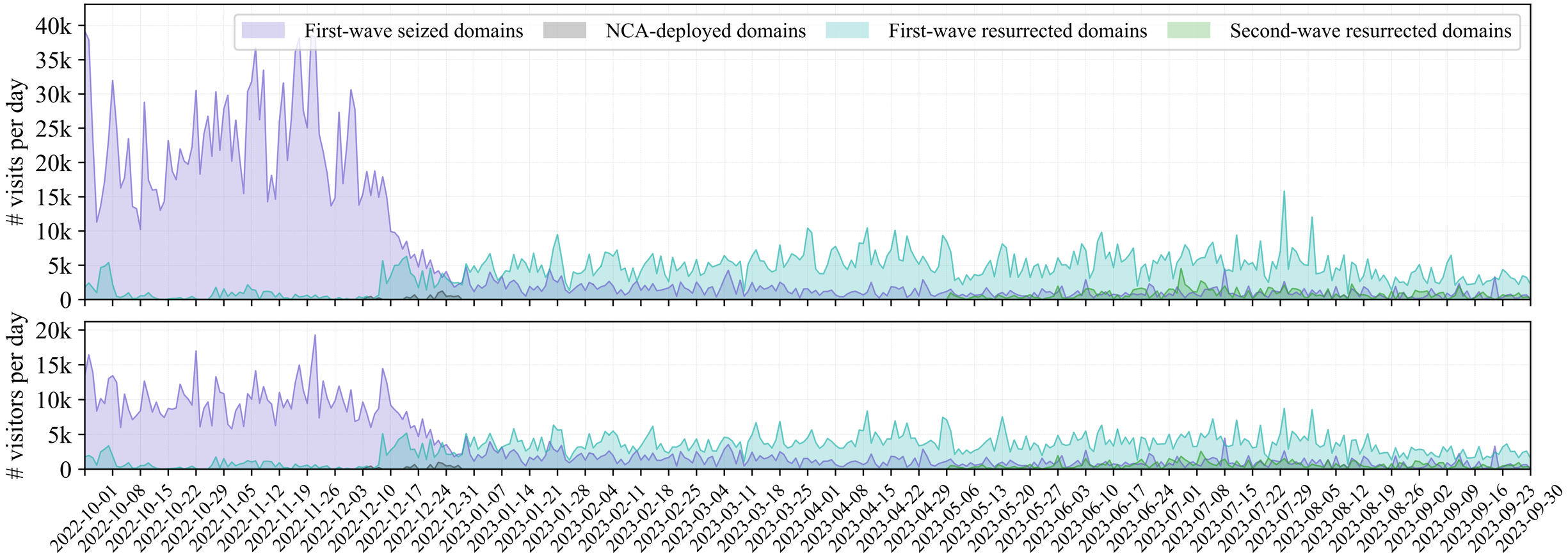
UNIVERSITY OF CAMBRIDGE

- Major booters provide APIs to others to create second-tier booters.
- Someone was still calling APIs without realising that their "big" booters had been seized.



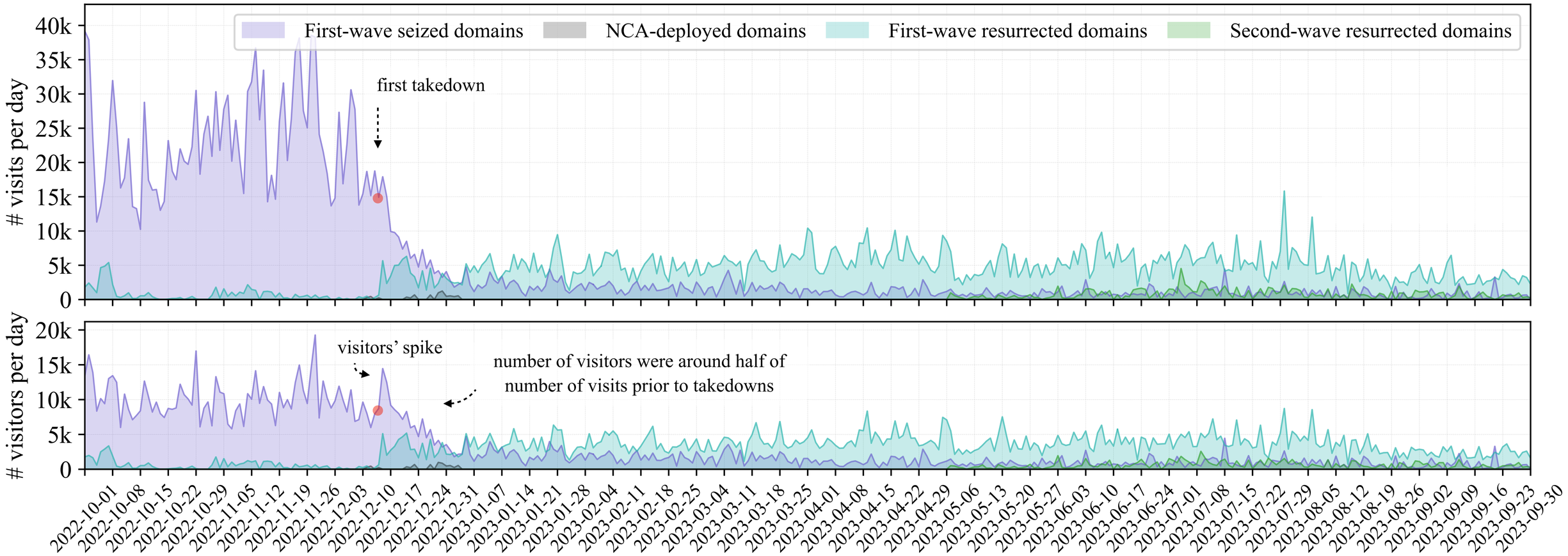
Disrupting the supply: traffic to seized booters declined

UNIVERSITY OF CAMBRIDGE



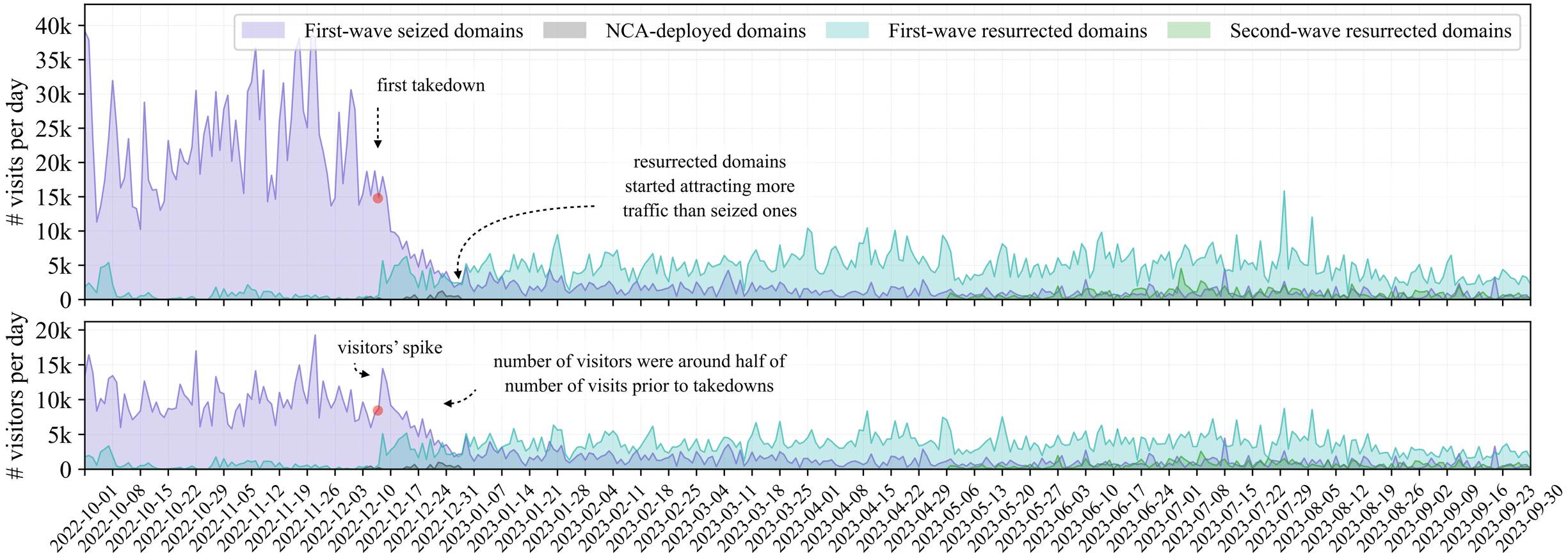
Disrupting the supply: traffic to seized booters declined

UNIVERSITY OF CAMBRIDGE



Disrupting the supply: traffic to seized booters declined

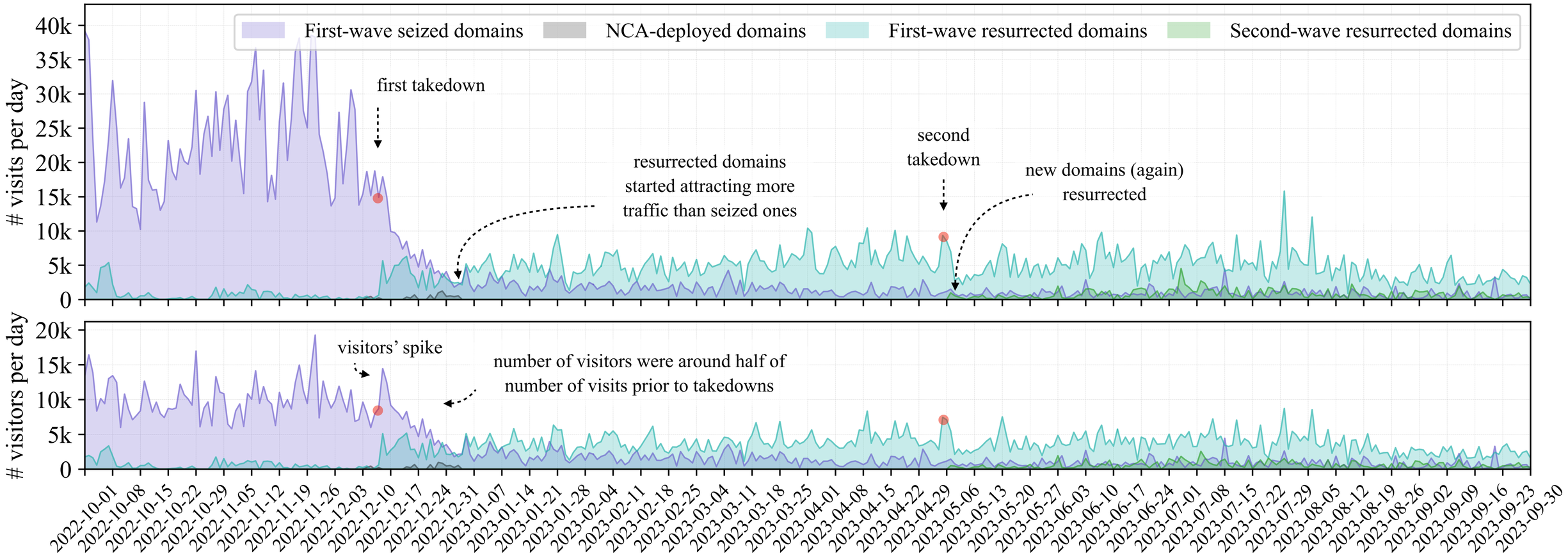
UNIVERSITY OF CAMBRIDGE



- First wave of takedowns: traffic was fragmented across resurrected domains, which grew quickly.

Disrupting the supply: traffic to seized booters declined

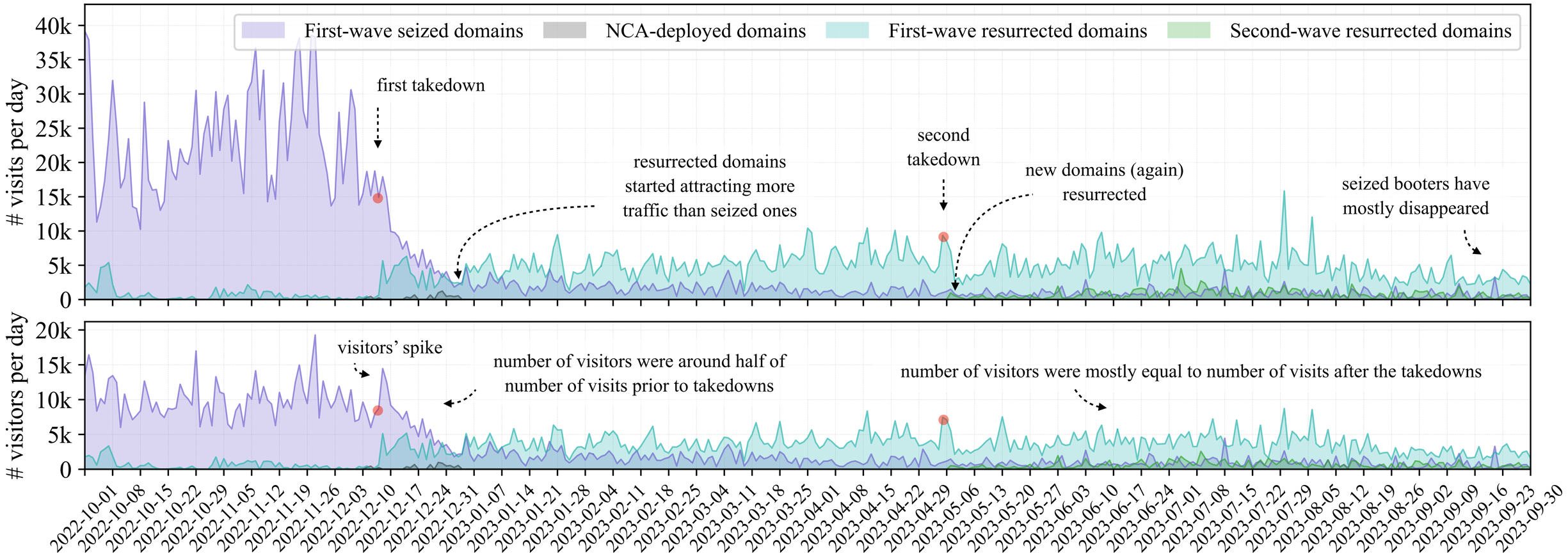
UNIVERSITY OF CAMBRIDGE



- First wave of takedowns: traffic was fragmented across resurrected domains, which grew quickly.
- Second wave of takedowns: minimal impact, resurrected domains show little growth in traffic.

Disrupting the supply: traffic to seized booters declined

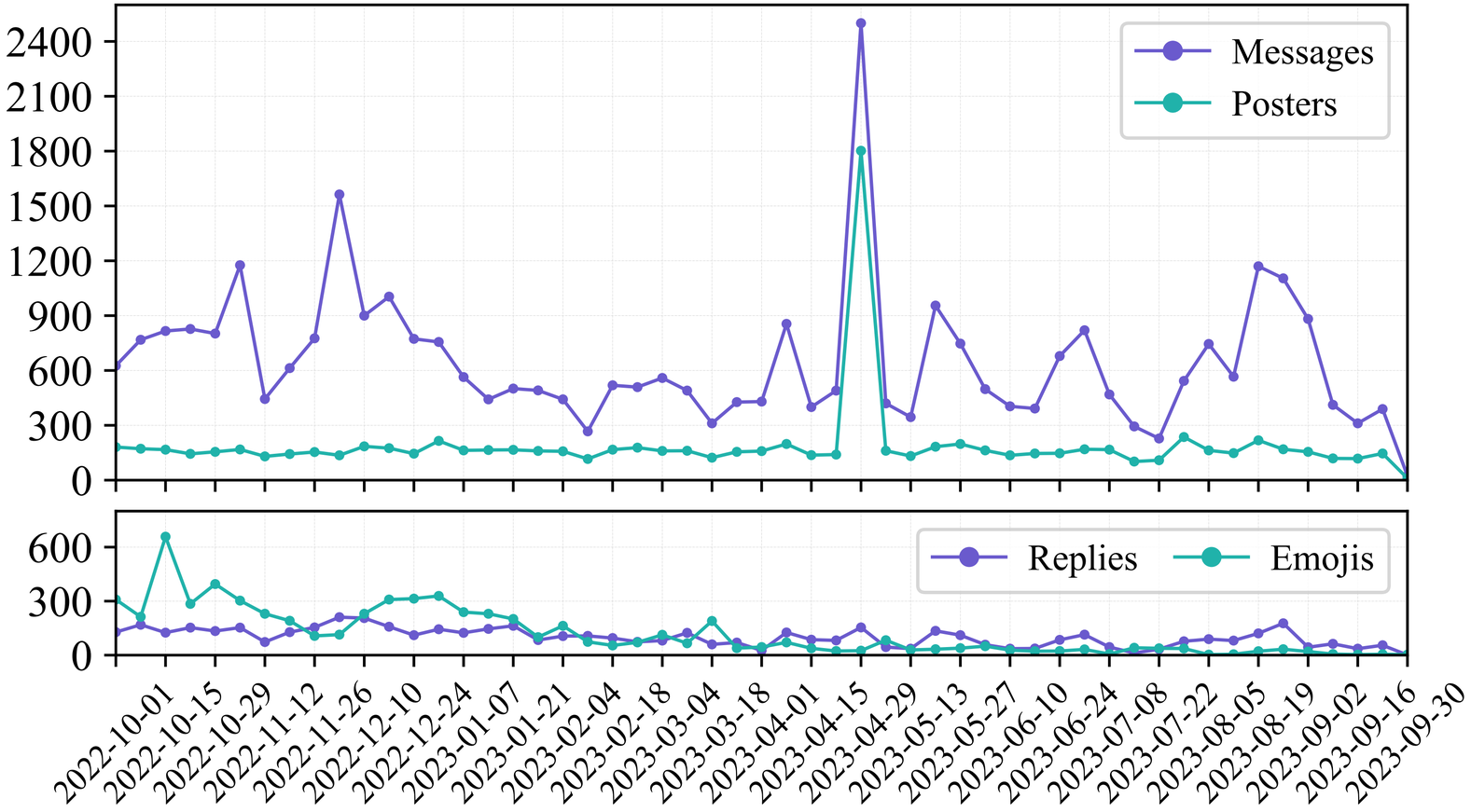
UNIVERSITY OF CAMBRIDGE



- First wave of takedowns: traffic was fragmented across resurrected domains, which grew quickly.
- Second wave of takedowns: minimal impact, resurrected domains show little growth in traffic.
- Overall, all resurrected domains have failed to attract as much traffic as before.

Telegram activity declined, and some operators left

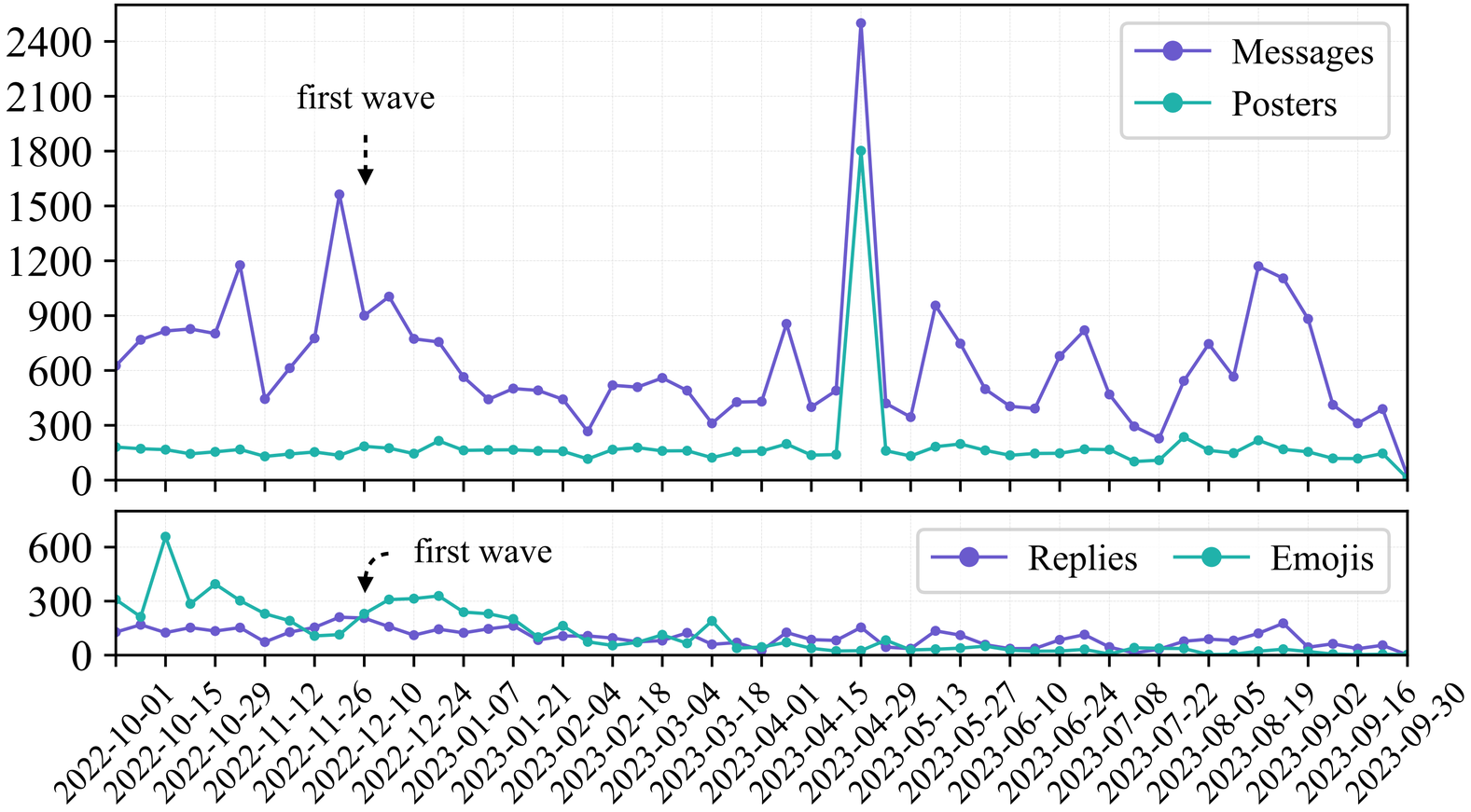
UNIVERSITY OF CAMBRIDGE



Number of messages and posting users on Telegram channels of all seized booters through the two waves of takedowns

Telegram activity declined, and some operators left

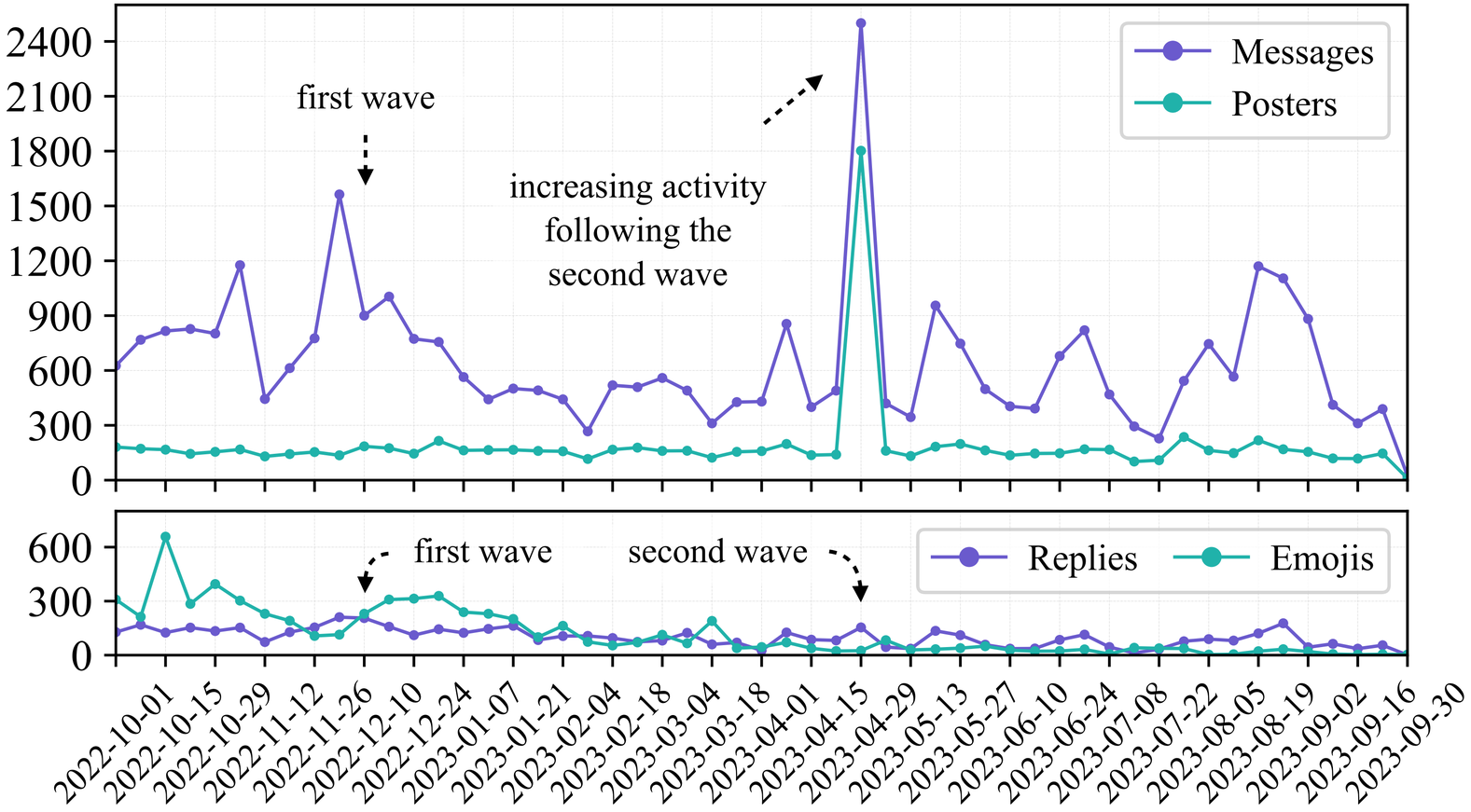
UNIVERSITY OF CAMBRIDGE



Number of messages and posting users on Telegram channels of all seized booters through the two waves of takedowns

Telegram activity declined, and some operators left

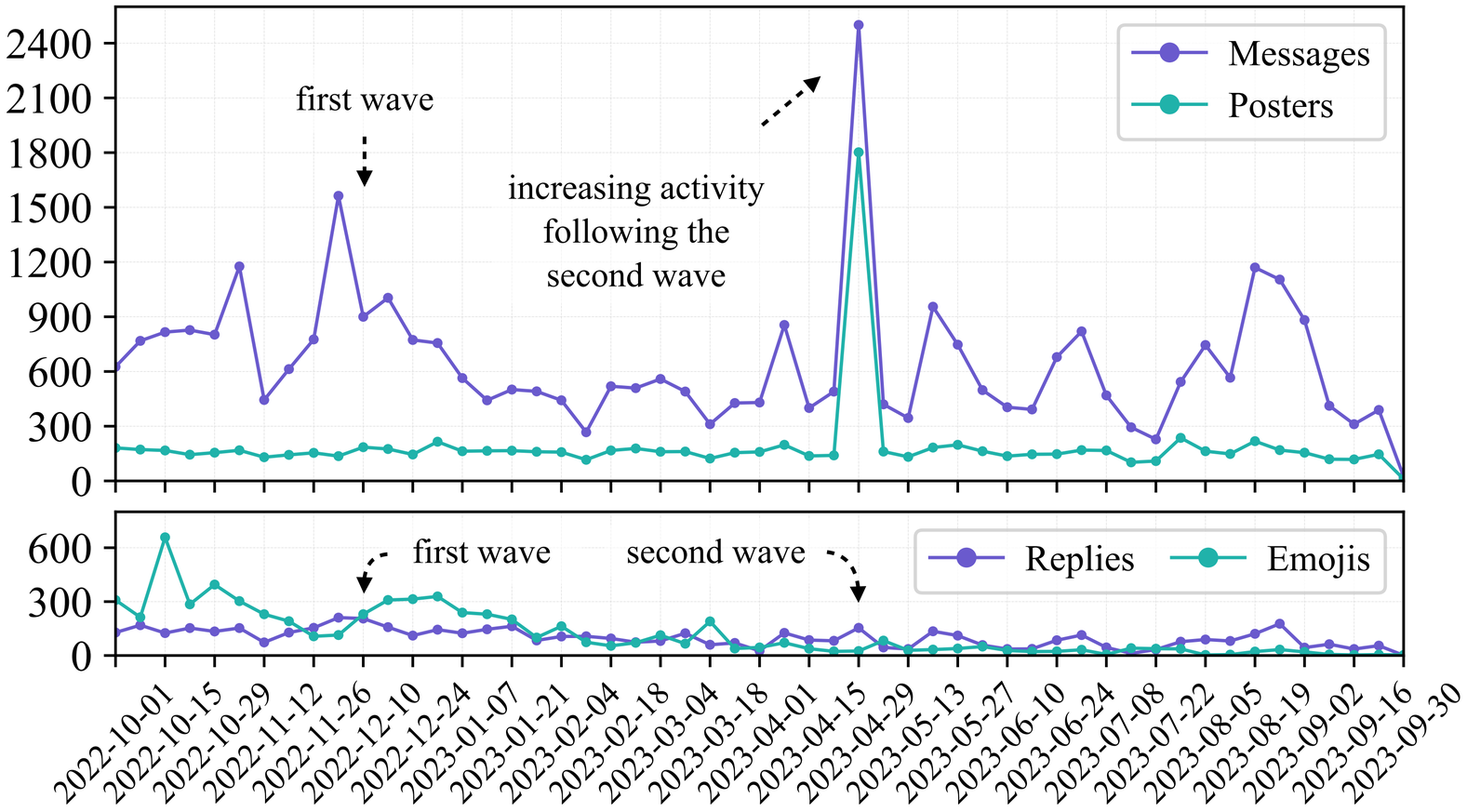
UNIVERSITY OF CAMBRIDGE



Number of messages and posting users on Telegram channels of all seized booters through the two waves of takedowns

Telegram activity declined, and some operators left

UNIVERSITY OF CAMBRIDGE



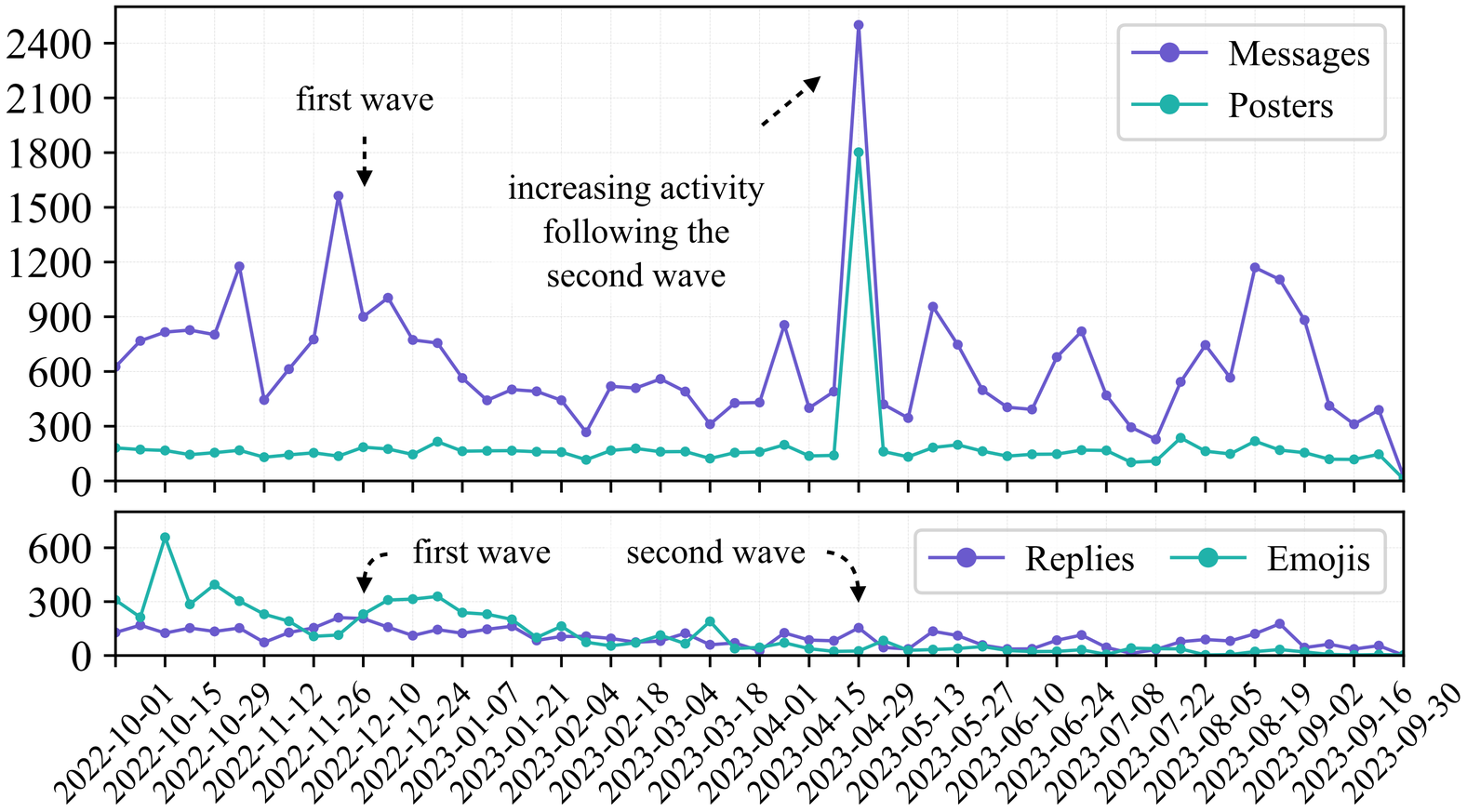
Number of messages and posting users on Telegram channels of all seized booters through the two waves of takedowns

We'll give you extra days on your plan due to unexpected downtime

All clients received a one-day extension

Telegram activity declined, and some operators left

UNIVERSITY OF CAMBRIDGE



Number of messages and posting users on Telegram channels of all seized booters through the two waves of takedowns

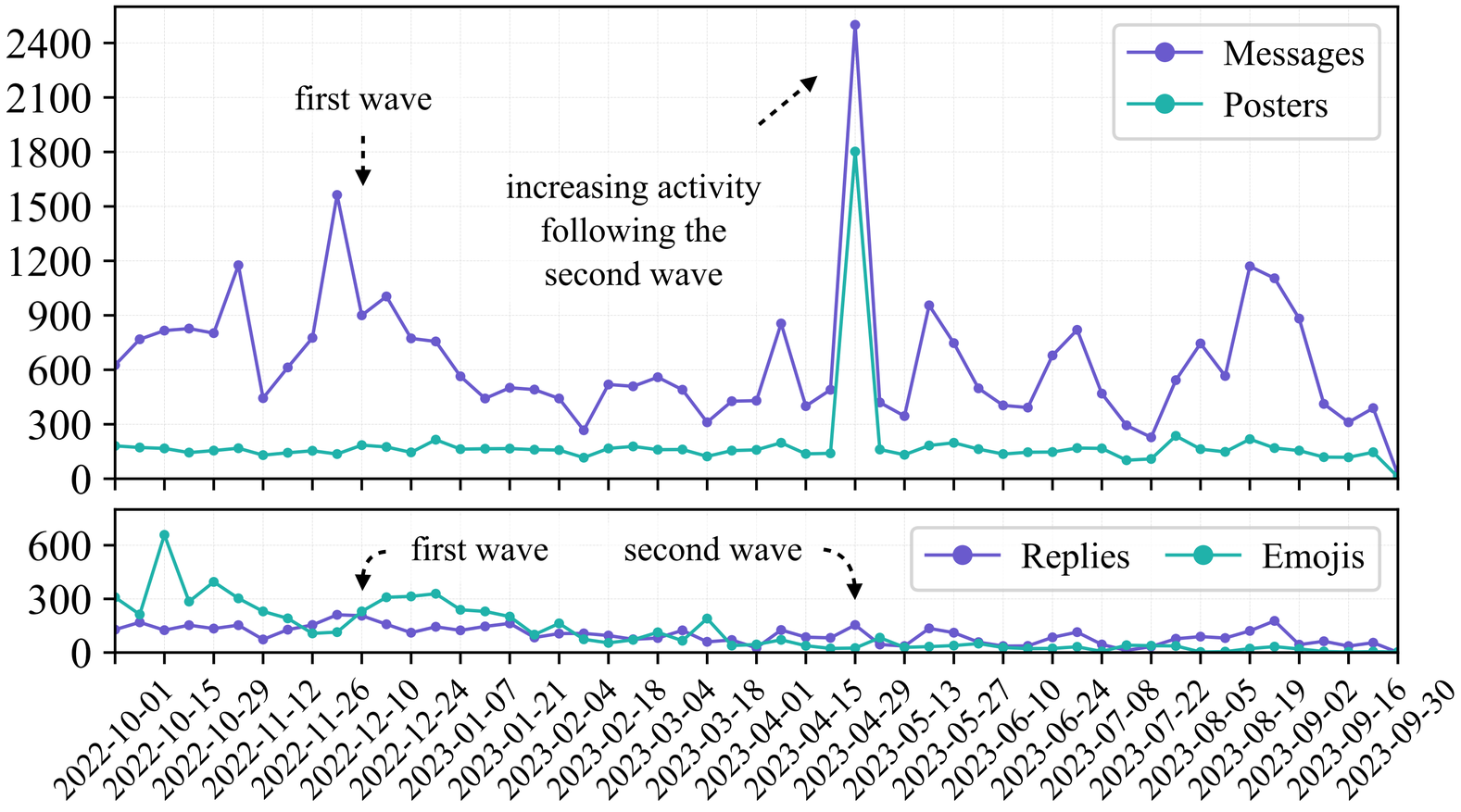
We'll give you extra days on your plan due to unexpected downtime

All clients received a one-day extension

Our current illegal income source is risky and unsustainable. police actions are happening, and many are coming in the future. [URL to the FBI seizure] – 15 December 2022

Telegram activity declined, and some operators left

UNIVERSITY OF CAMBRIDGE



Number of messages and posting users on Telegram channels of all seized booters through the two waves of takedowns

We'll give you extra days on your plan due to unexpected downtime

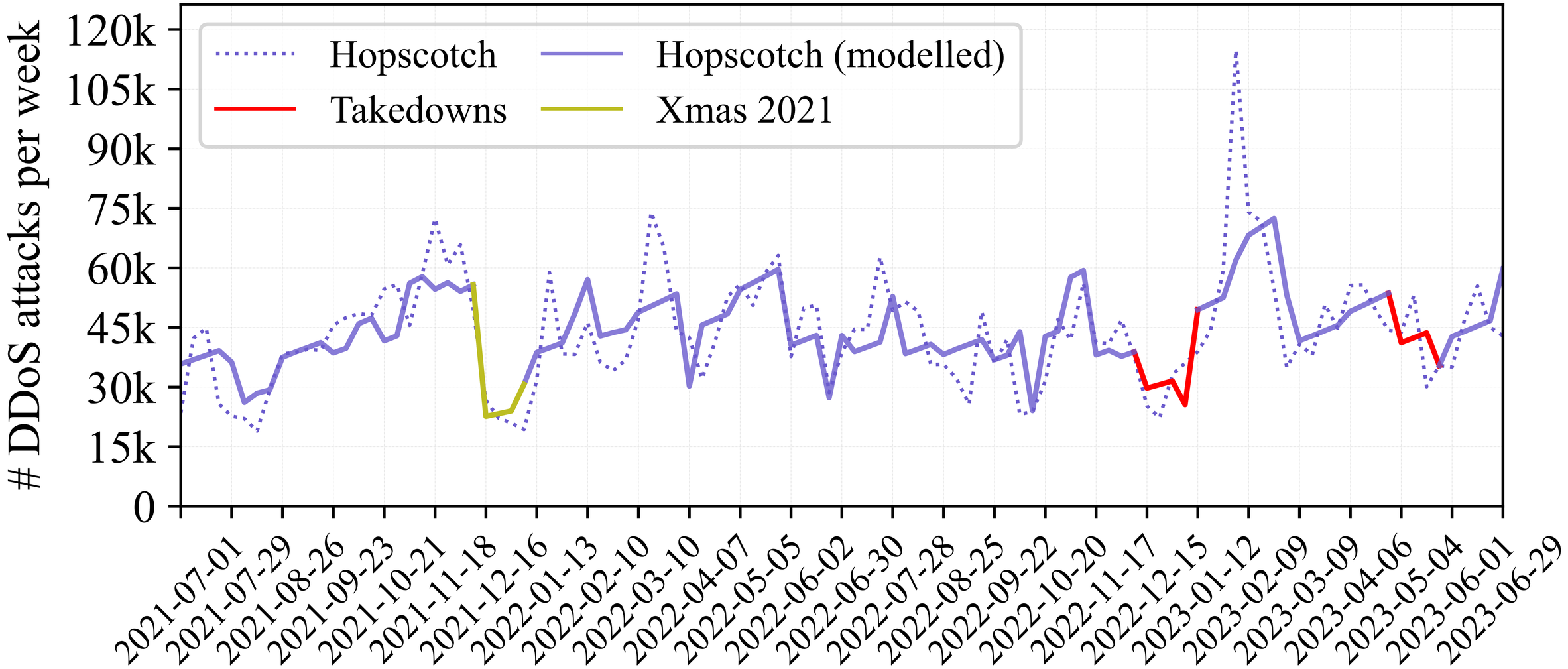
All clients received a one-day extension

Our current illegal income source is risky and unsustainable. police actions are happening, and many are coming in the future. [URL to the FBI seizure] – 15 December 2022

Looking for a good developer? I'm currently available and ready to tackle your project, big or small. I have experience with Golang, Rust, C, C++, Python, JavaScript, and other languages. Don't hesitate to send me a message to discuss your needs. (Small projects are very cheap!) – 19 May 2023

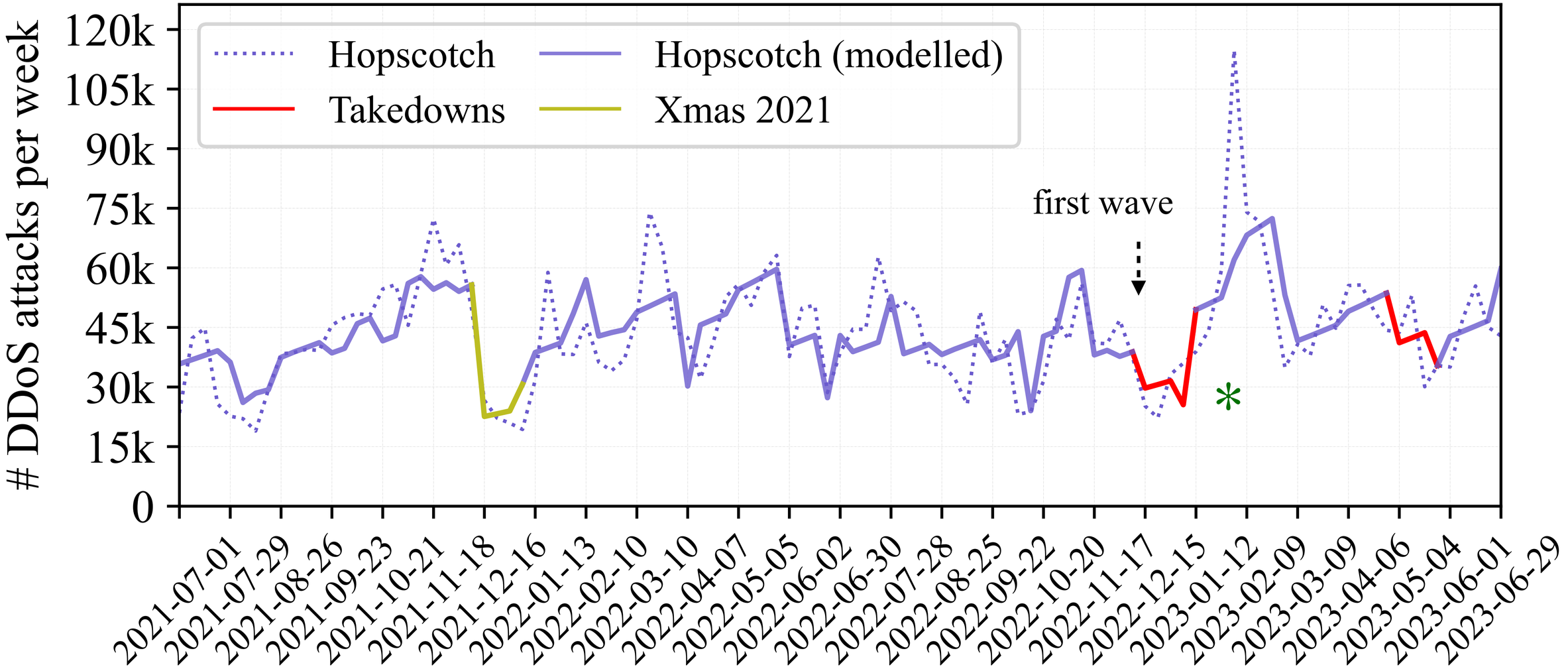
DDoS attack volumes — Hopscotch view (UDP-based)

UNIVERSITY OF CAMBRIDGE



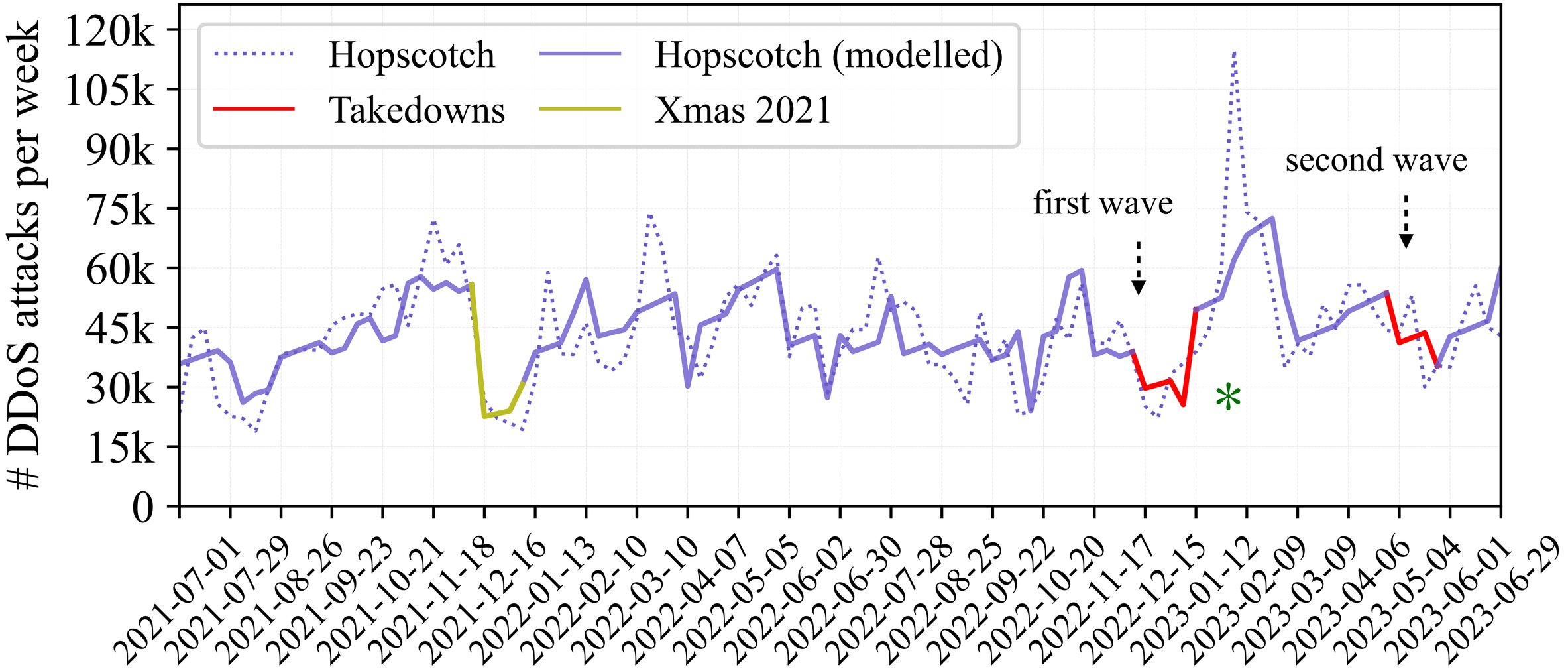
DDoS attack volumes — Hopscotch view (UDP-based)

UNIVERSITY OF CAMBRIDGE



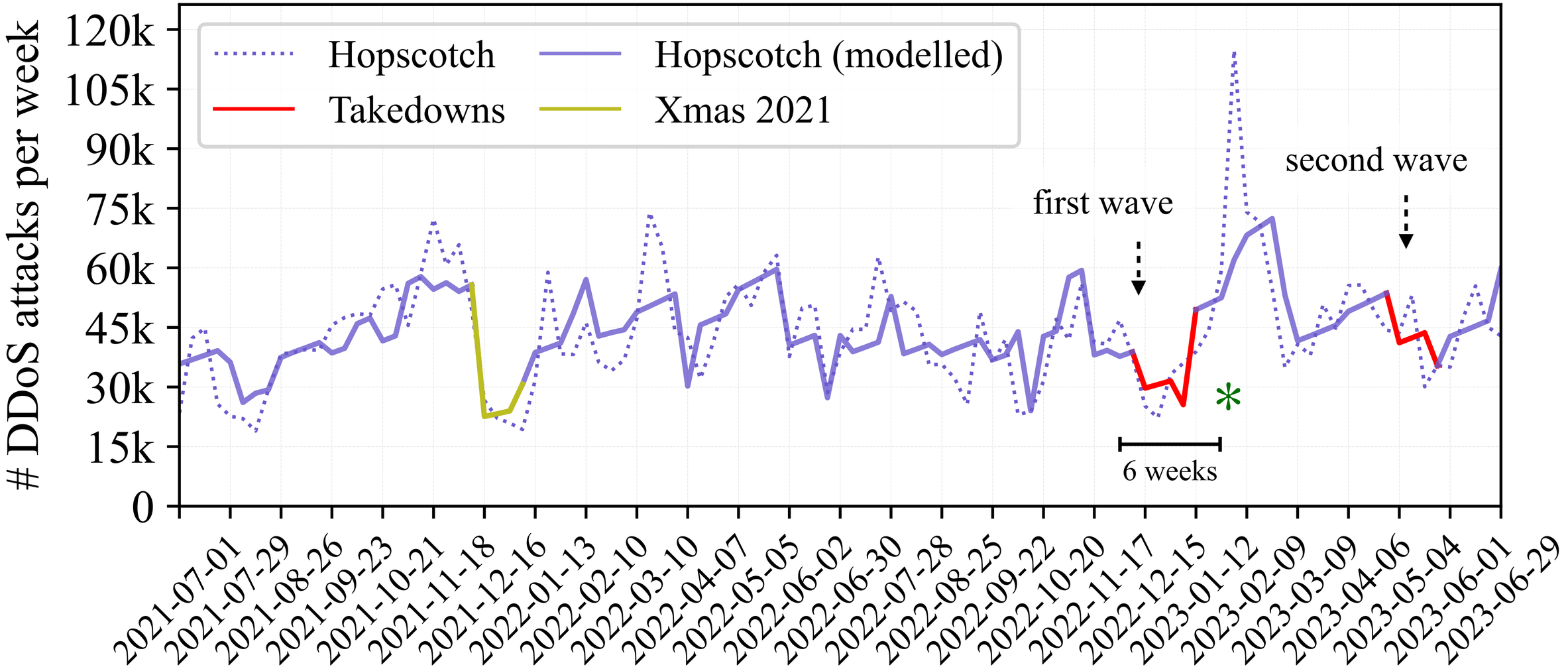
DDoS attack volumes — Hopscotch view (UDP-based)

UNIVERSITY OF CAMBRIDGE



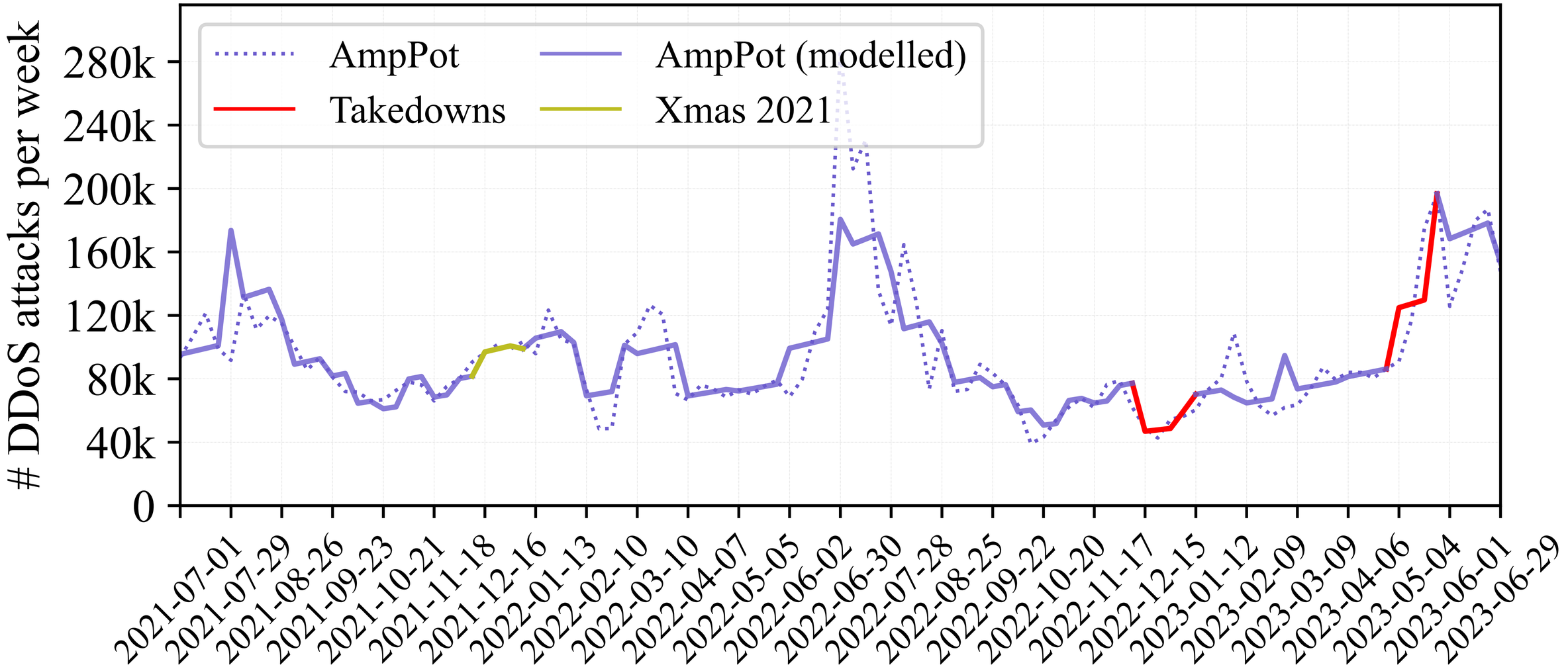
DDoS attack volumes — Hopscotch view (UDP-based)

UNIVERSITY OF CAMBRIDGE



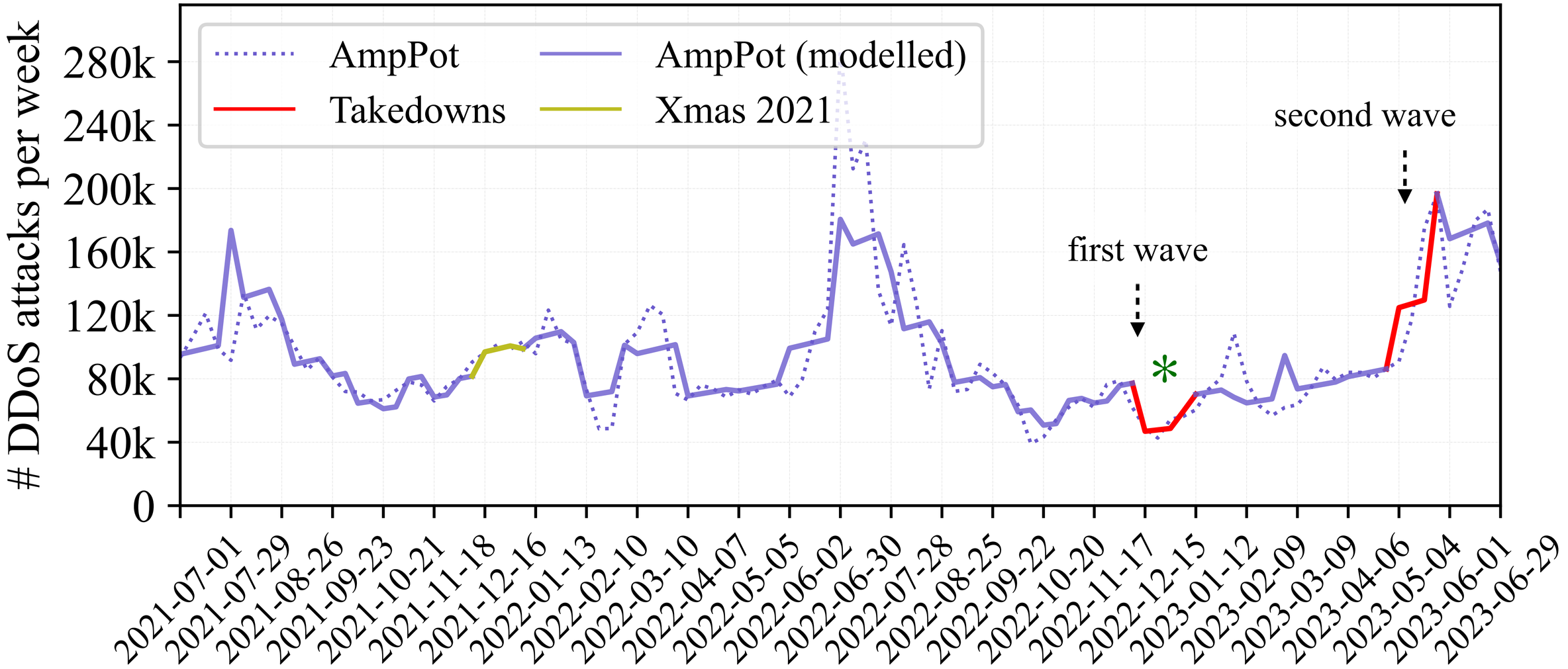
DDoS attack volumes — AmpPot view (UDP-based)

UNIVERSITY OF CAMBRIDGE



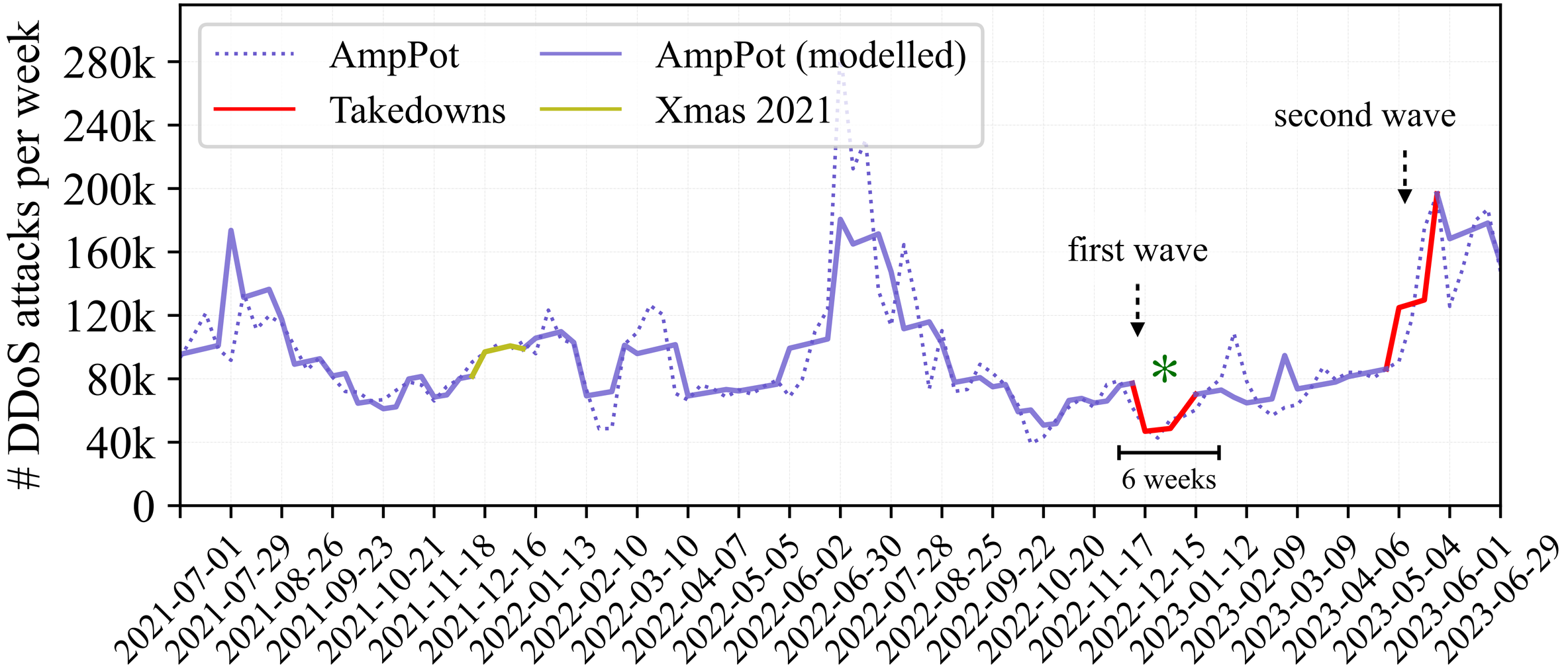
DDoS attack volumes — AmpPot view (UDP-based)

UNIVERSITY OF CAMBRIDGE



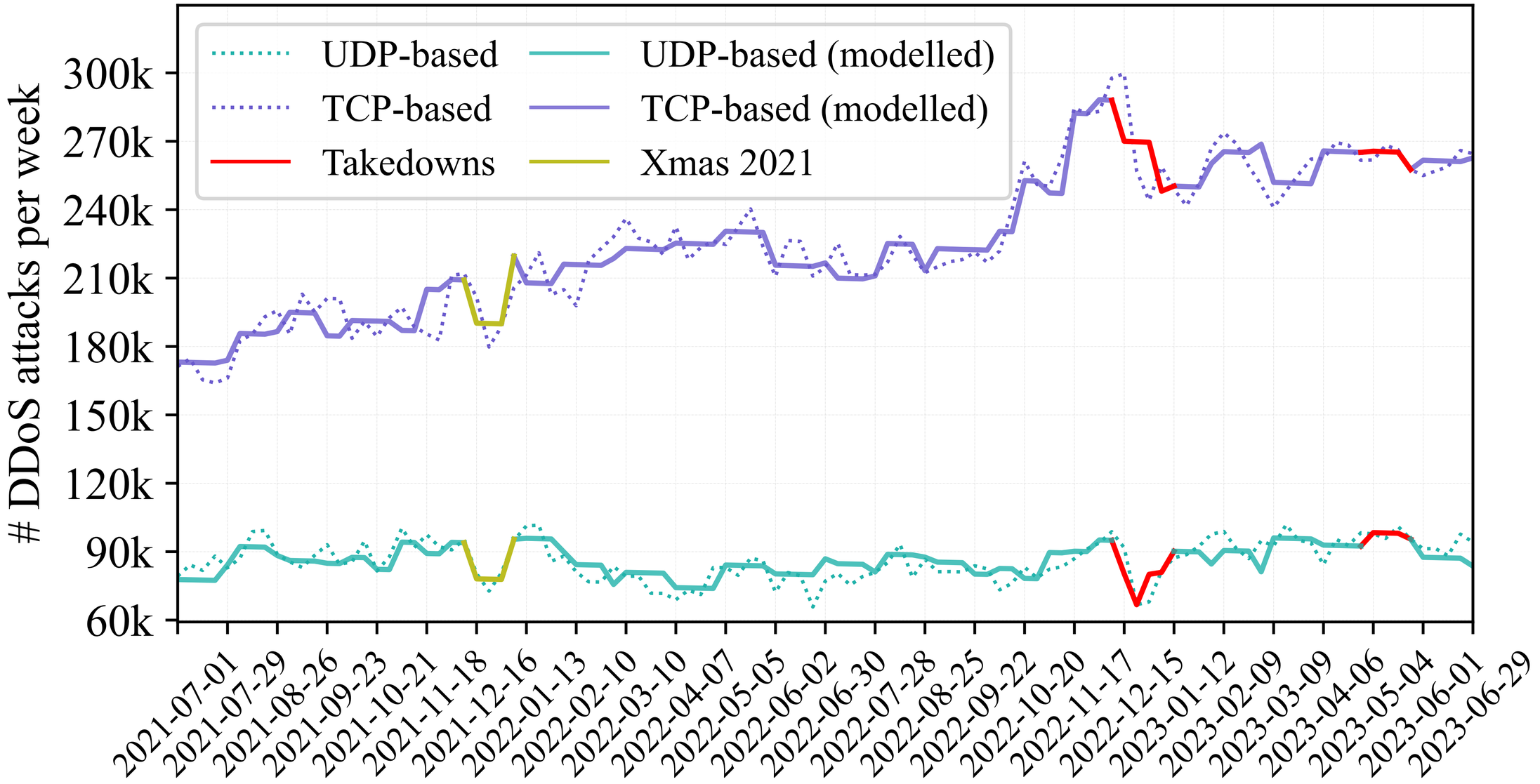
DDoS attack volumes — AmpPot view (UDP-based)

UNIVERSITY OF CAMBRIDGE



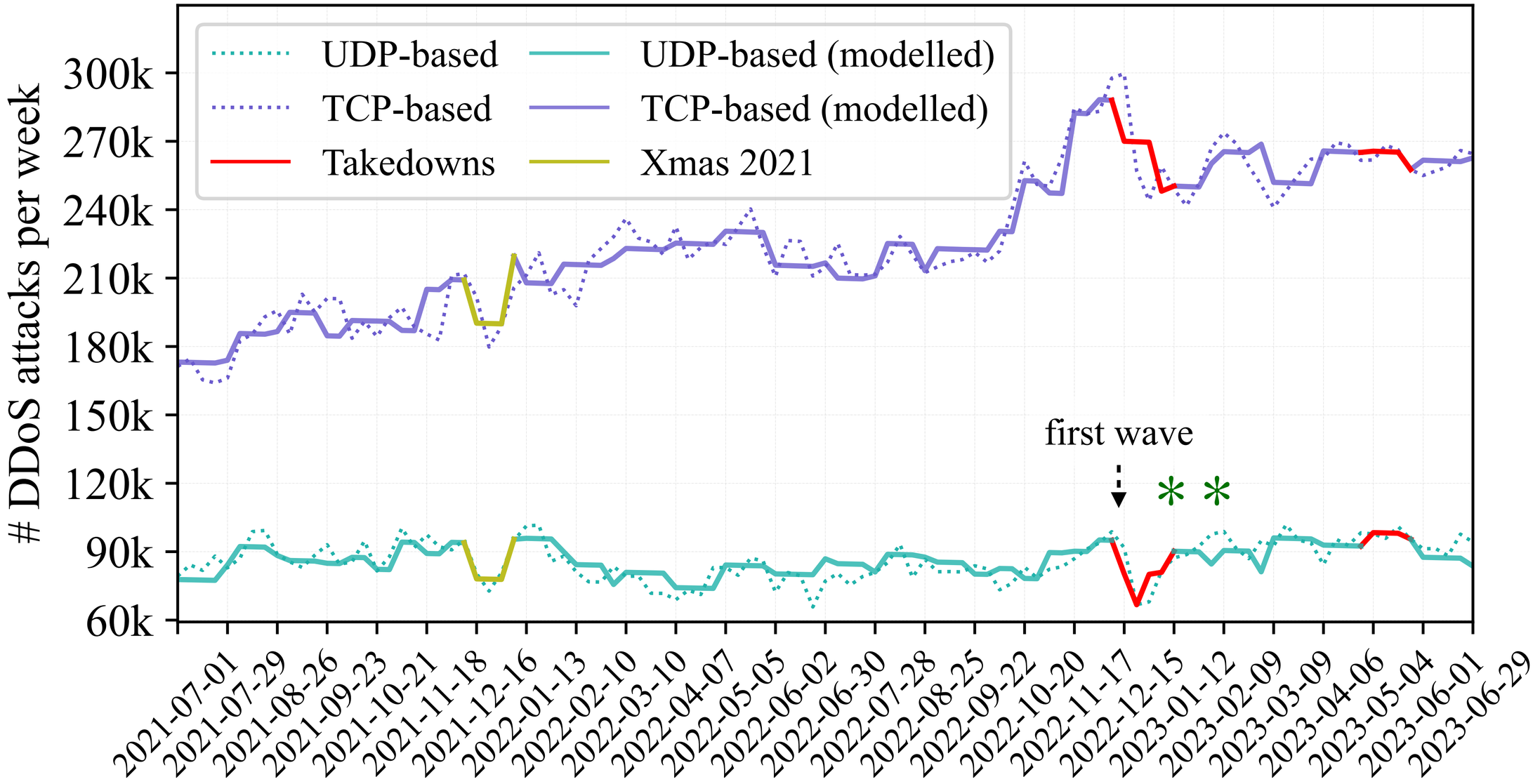
DDoS attack volumes — Netscout view

UNIVERSITY OF CAMBRIDGE



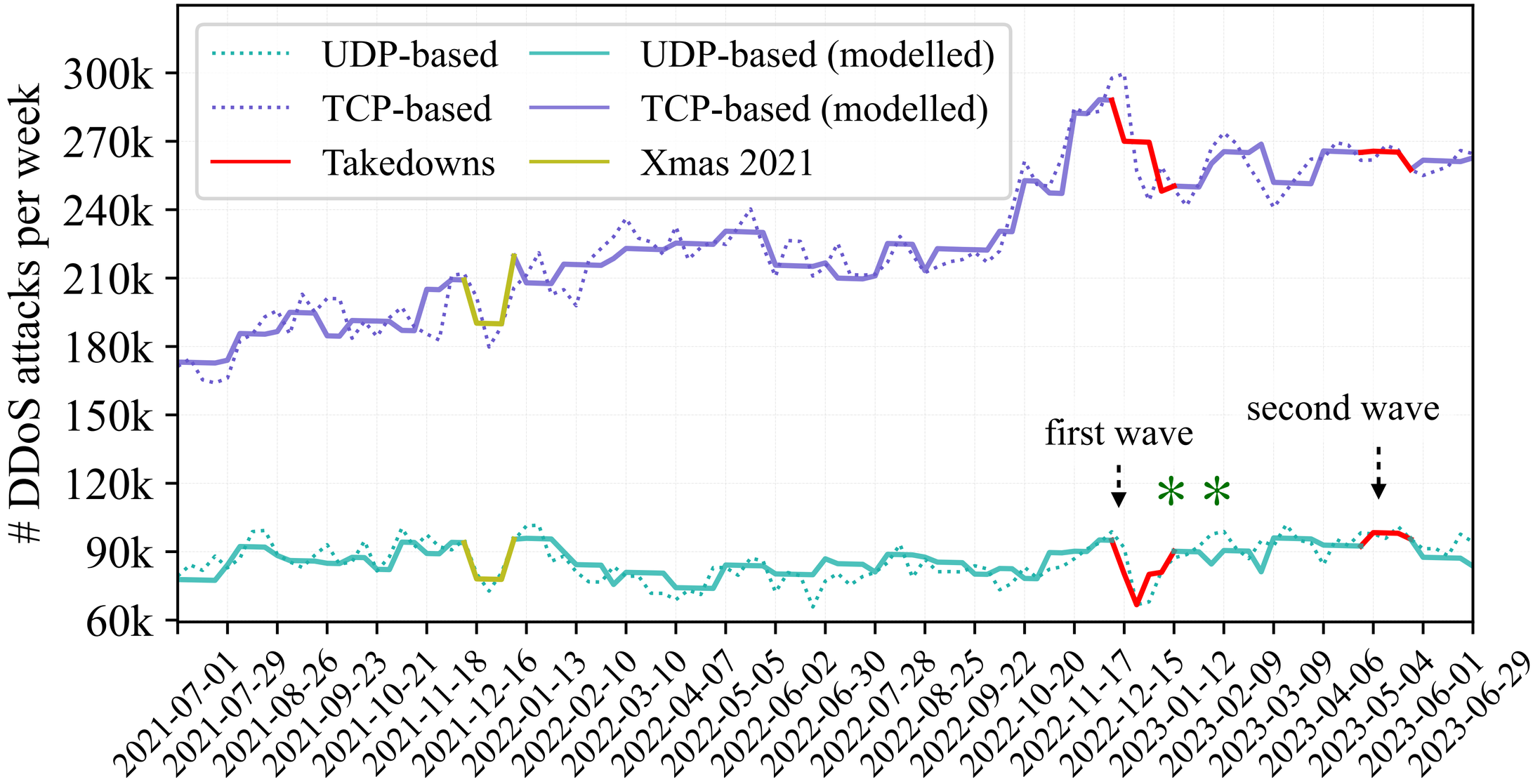
DDoS attack volumes — Netscout view

UNIVERSITY OF CAMBRIDGE



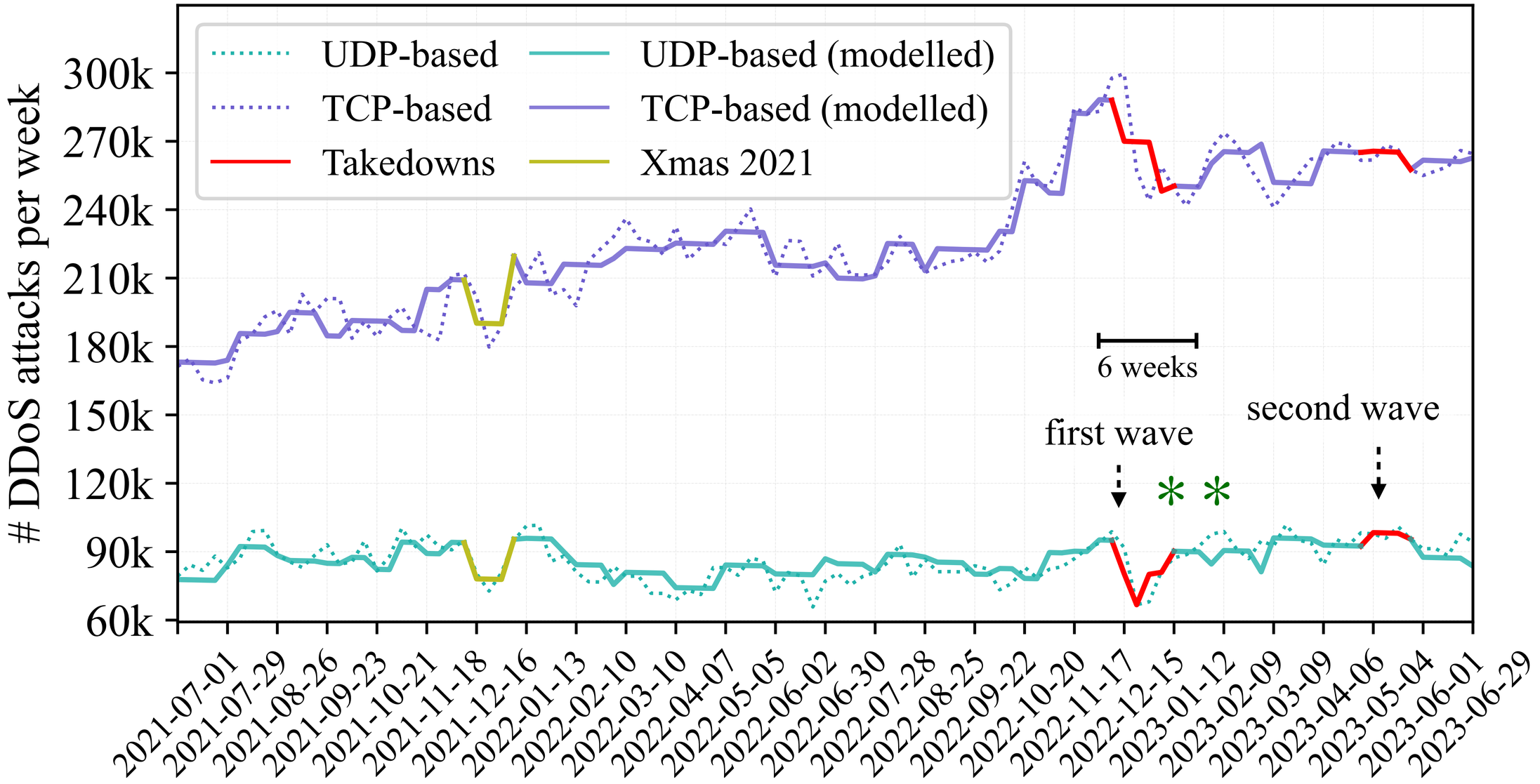
DDoS attack volumes — Netscout view

UNIVERSITY OF CAMBRIDGE



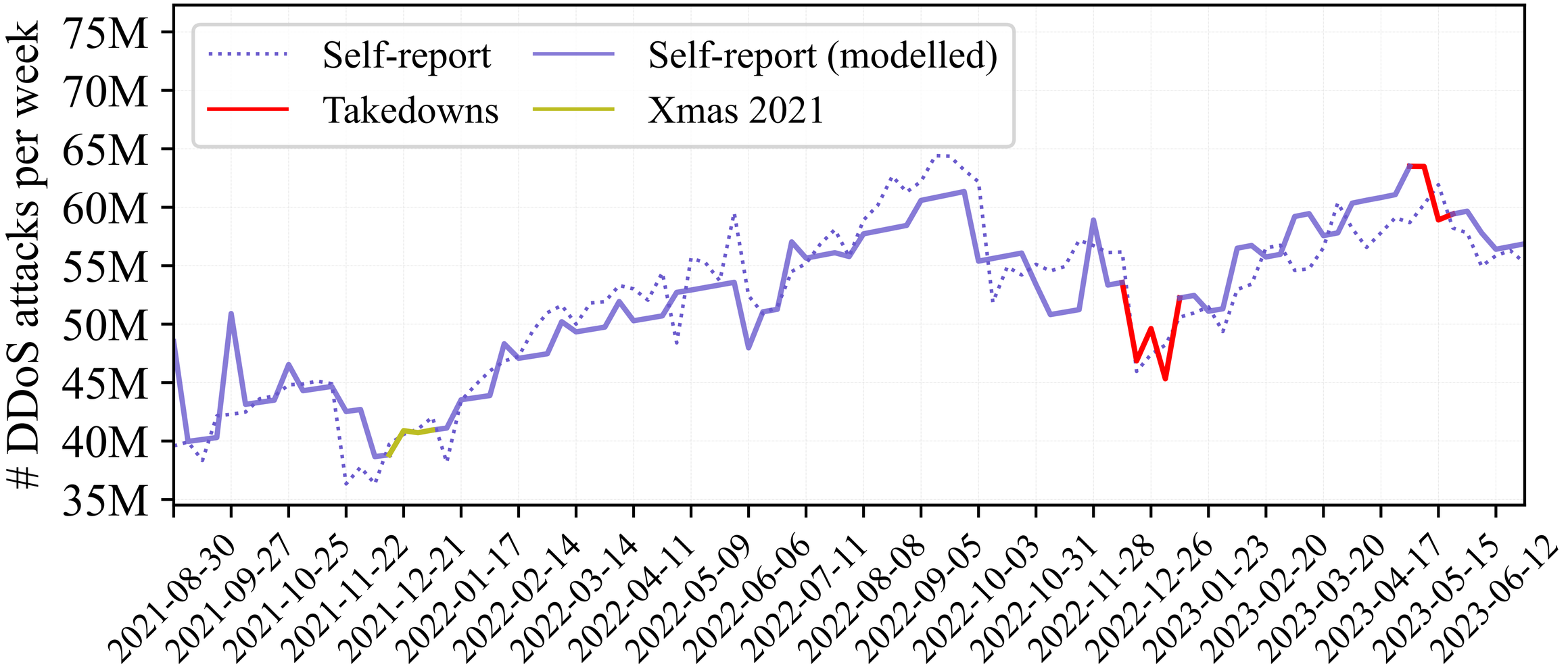
DDoS attack volumes — Netscout view

UNIVERSITY OF CAMBRIDGE



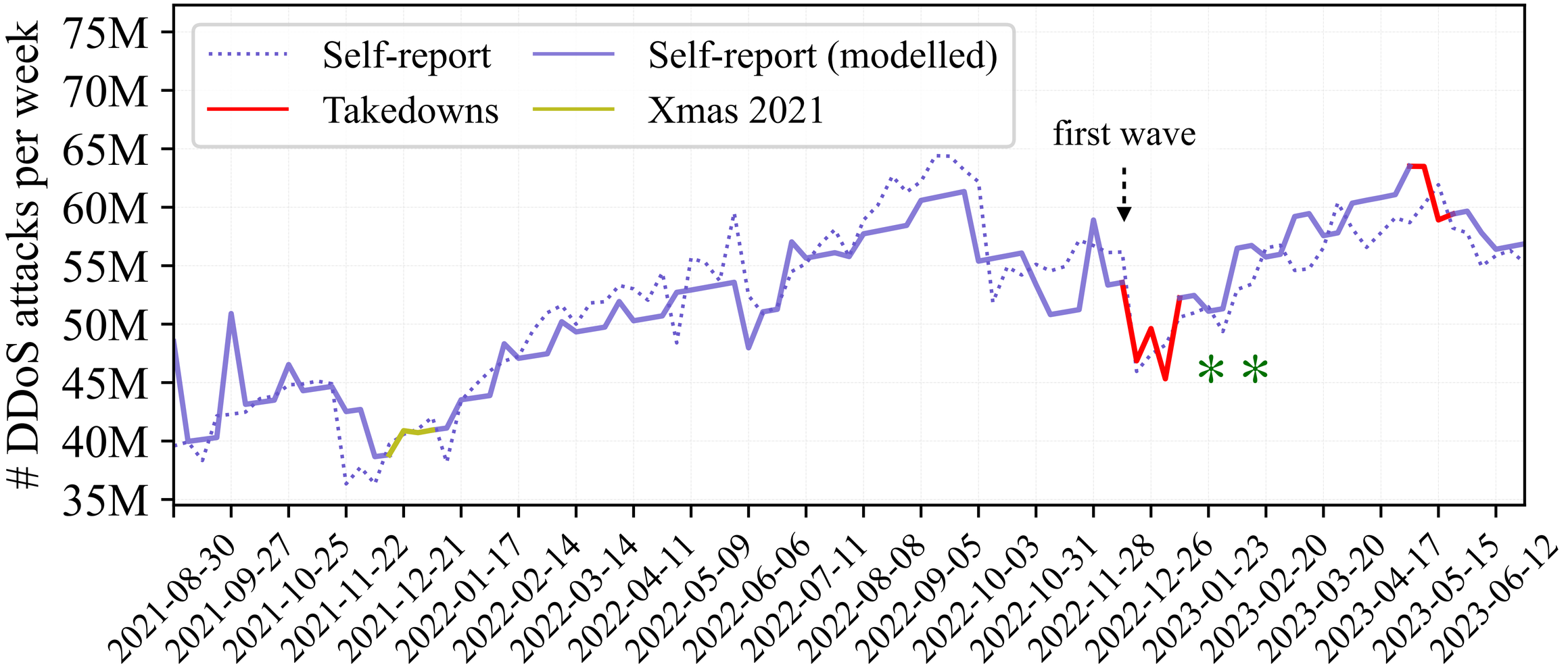
DDoS attack volumes — Self-reported statistics

UNIVERSITY OF CAMBRIDGE



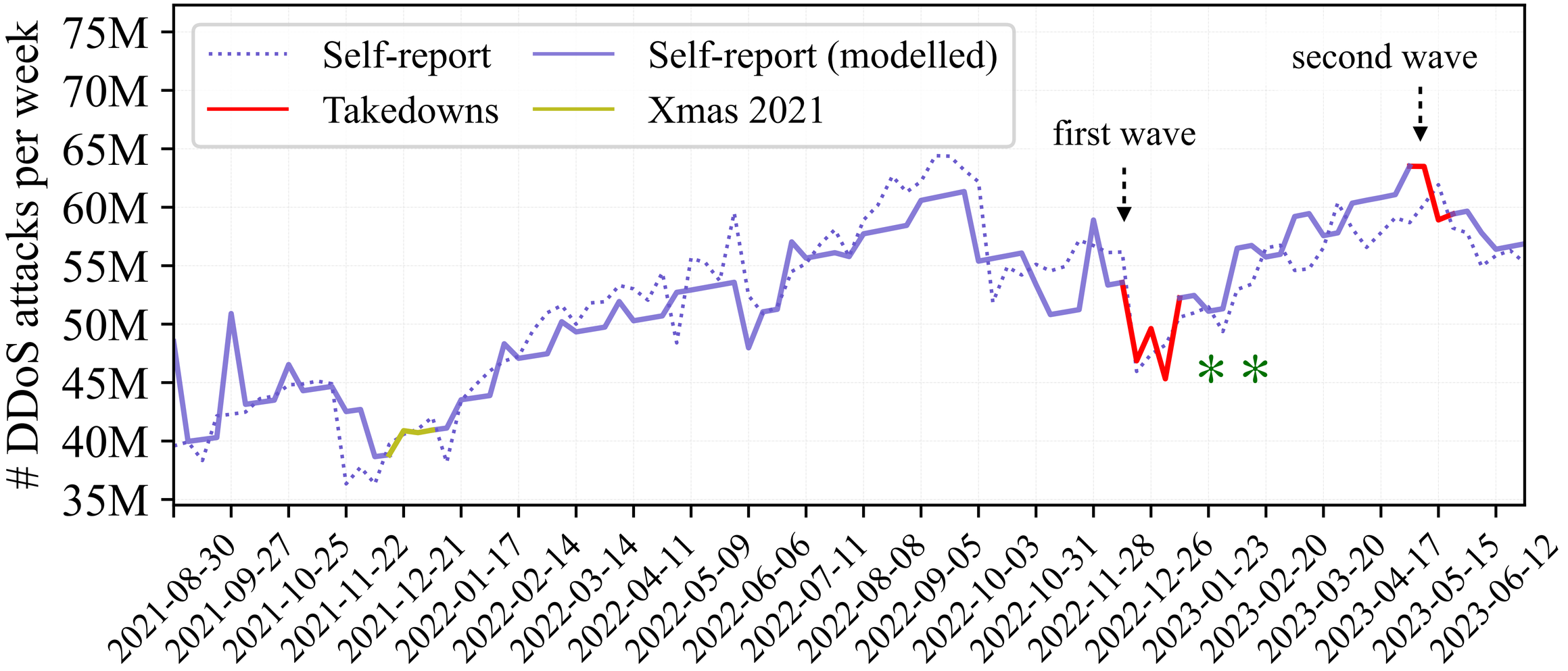
DDoS attack volumes — Self-reported statistics

UNIVERSITY OF CAMBRIDGE



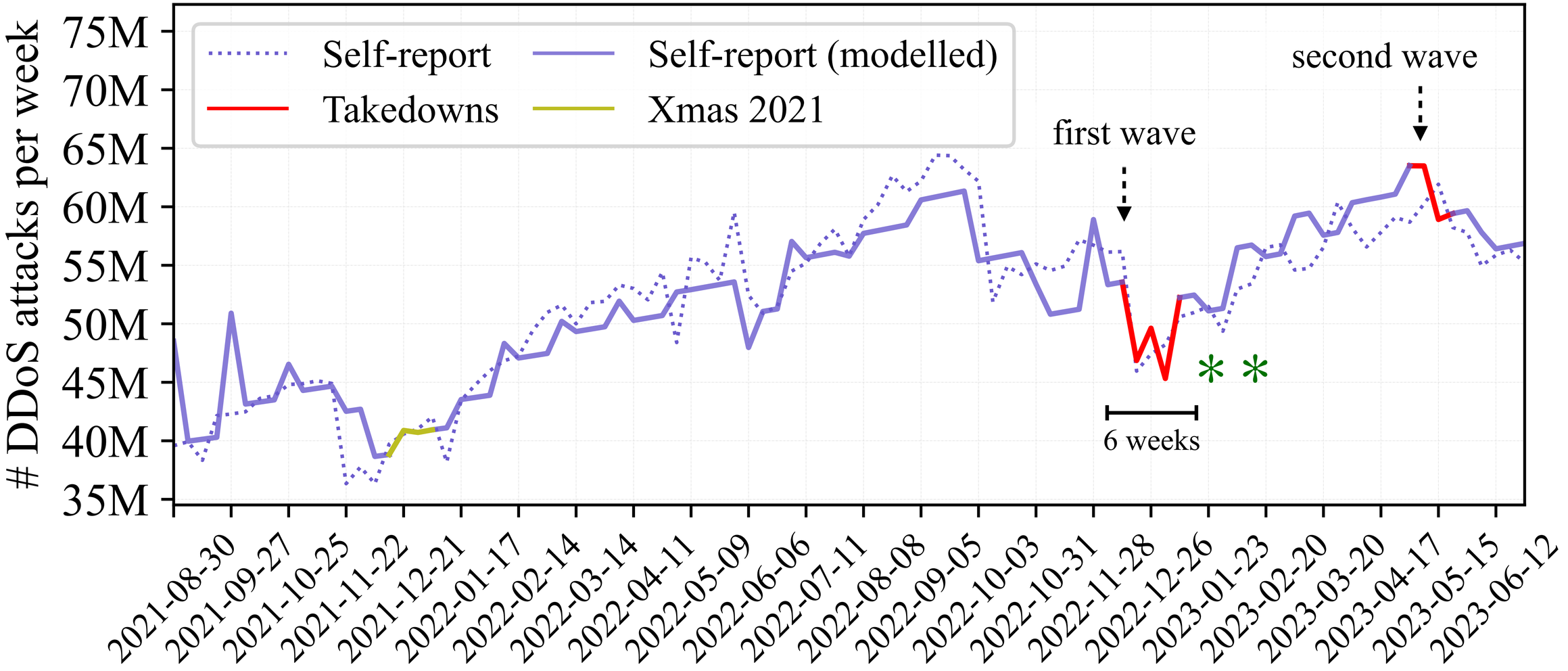
DDoS attack volumes — Self-reported statistics

UNIVERSITY OF CAMBRIDGE



DDoS attack volumes — Self-reported statistics

UNIVERSITY OF CAMBRIDGE



Concluding remarks

- The market was relatively fragile at the beginning: all resurrected domains attracted far less traffic than before, suggesting a positive takedown impact.
- UDP-based attacks (often attributed to booters) were significantly impacted; however, it took only about six weeks for the global DDoS attacks to recover.

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

Anh V. Vu
University of Cambridge
anh.vu@cl.cam.ac.uk

Ben Collier
University of Edinburgh
ben.collier@ed.ac.uk

Daniel R. Thomas
University of Strathclyde
d.thomas@strath.ac.uk

John Kristoff
University of Illinois Chicago
jkrist3@uic.edu

Richard Clayton
University of Cambridge
richard.clayton@cl.cam.ac.uk

Alice Hutchings
University of Cambridge
alice.hutchings@cl.cam.ac.uk

Abstract

Law enforcement and private-sector partners have in recent years conducted various interventions to disrupt the DDoS-for-hire market. Drawing on multiple quantitative datasets, including web traffic and ground-truth visits to seized websites, millions of DDoS attack records from academic, industry, and self-reported statistics, along with chats on underground forums and Telegram channels, we assess the effects of an ongoing global intervention against DDoS-for-hire services since December 2022. This is the most extensive booter takedown to date conducted, combining targeting infrastructure with digital influence tactics in a concerted effort by law enforcement across several countries with two waves of website takedowns and the use of deceptive domains. We found over half of the seized sites in the first wave returned within a median of one day, while all booters seized in the second wave returned within a median of two days. Re-emerged booter domains, despite closely resembling old ones, struggled to attract visitors (80–90% traffic reduction). While the first wave cut the global DDoS attack volume by 20–40% with a statistically significant effect specifically on UDP-based DDoS attacks (commonly attributed to booters), the impact of the second wave appeared minimal. Underground discussions indicated a cumulative impact, leading to changes in user perceptions of safety and causing some operators to leave the market. Despite the extensive intervention efforts, all DDoS datasets consistently suggest that the illicit market is fairly resilient, with an overall short-lived effect on the global DDoS attack volume lasting only around six weeks.

1 Introduction

The economic and social dynamics of the cybercrime ecosystem have fundamentally changed over the past two decades. There have been significant shifts in both the scale and nature of harmful and illicit activity resulting from the increasing industrialisation of economic cybercrime. Individuals using simple methods remain an issue, but they now have the option of using fully-fledged commercial service offerings. Off-the-shelf toolkits and attack-as-a-service infrastructure are routinely advertised, rented, and sold through a variety of open and private online marketplaces [1–3]. Each stage of this evolution has drastically reduced the skill and cost barriers for users to participate in what were previously considered more 'technical' forms of online harm [4].

The as-a-service model facilitates largely underreported high-volume but low-value online crimes, which may avoid public scrutiny and law enforcement attention. For example, starting at a few dollars per month, online markets for DDoS attacks (so-called *booters* or *stressers*) allow unskilled actors to flood online services with unwanted traffic, knocking systems without robust security offline [5]. Booter operators may justify their services as testing server resilience, but their primary uses and methods are illegal [6].

The entrepreneurial, service-based nature of booters makes them vulnerable to targeted interventions. Although individual arrests may be generally ineffective in industrialised market crime economies as they aid competitors, the economic forces driving these markets tend to lead to the centralisation of the infrastructure and supportive work on which they depend (through well-understood efficiencies and network externalities). Booter infrastructure consolidation therefore presents an apposite target for disruption activities. In a major takedown event in December 2018, 15 of the largest booters were seized in an international law enforcement effort [7]. However, the effect was relatively short-lived, with DDoS attack volumes recovering a few weeks later [8, 9].

Building on practitioner learning and academic analysis of previous efforts, a further major intervention was conducted from late 2022, combining targeting infrastructure with influence operation components: 49 booter domains were seized in December 2022 (the first wave) [10], 13 domains were seized in May 2023 (the second wave) [11], and several deceptive sites were set up by law enforcement. This campaign has been much greater in scale and more persistent than the one four years earlier, leading us to ask: how effective might it be?

There are several material aspects of online crime that make

UNIVERSITY OF CAMBRIDGE · THE UNIVERSITY of EDINBURGH · University of Strathclyde Glasgow · UIC UNIVERSITY OF ILLINOIS CHICAGO

Anh V. Vu — anh.vu@cst.cam.ac.uk

Concluding remarks

- The market was relatively fragile at the beginning: all resurrected domains attracted far less traffic than before, suggesting a positive takedown impact.
- UDP-based attacks (often attributed to booters) were significantly impacted; however, it took only about six weeks for the global DDoS attacks to recover.
- The overall intervention impact appears to be rather short-lived. Suppressing the supply side alone may not suffice, as demand likely persists in the long run.
- Data access: datarequest@cambridgecybercrime.uk

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

Anh V. Vu
University of Cambridge
anh.vu@cl.cam.ac.uk

Ben Collier
University of Edinburgh
ben.collier@ed.ac.uk

Daniel R. Thomas
University of Strathclyde
d.thomas@strath.ac.uk

John Kristoff
University of Illinois Chicago
jkrist3@uic.edu

Richard Clayton
University of Cambridge
richard.clayton@cl.cam.ac.uk

Alice Hutchings
University of Cambridge
alice.hutchings@cl.cam.ac.uk

Abstract

Law enforcement and private-sector partners have in recent years conducted various interventions to disrupt the DDoS-for-hire market. Drawing on multiple quantitative datasets, including web traffic and ground-truth visits to seized websites, millions of DDoS attack records from academic, industry, and self-reported statistics, along with chats on underground forums and Telegram channels, we assess the effects of an ongoing global intervention against DDoS-for-hire services since December 2022. This is the most extensive booter takedown to date conducted, combining targeting infrastructure with digital influence tactics in a concerted effort by law enforcement across several countries with two waves of website takedowns and the use of deceptive domains. We found over half of the seized sites in the first wave returned within a median of one day, while all booters seized in the second wave returned within a median of two days. Re-emerged booter domains, despite closely resembling old ones, struggled to attract visitors (80–90% traffic reduction). While the first wave cut the global DDoS attack volume by 20–40% with a statistically significant effect specifically on UDP-based DDoS attacks (commonly attributed to booters), the impact of the second wave appeared minimal. Underground discussions indicated a cumulative impact, leading to changes in user perceptions of safety and causing some operators to leave the market. Despite the extensive intervention efforts, all DDoS datasets consistently suggest that the illicit market is fairly resilient, with an overall short-lived effect on the global DDoS attack volume lasting only around six weeks.

1 Introduction

The economic and social dynamics of the cybercrime ecosystem have fundamentally changed over the past two decades. There have been significant shifts in both the scale and nature of harmful and illicit activity resulting from the increasing industrialisation of economic cybercrime. Individuals using simple methods remain an issue, but they now have the option of using fully-fledged commercial service offerings. Off-the-shelf toolkits and attack-as-a-service infrastructure are routinely advertised, rented, and sold through a variety of open and private online marketplaces [1–3]. Each stage of this evolution has drastically reduced the skill and cost barriers for users to participate in what were previously considered more 'technical' forms of online harm [4].

The as-a-service model facilitates largely underreported high-volume but low-value online crimes, which may avoid public scrutiny and law enforcement attention. For example, starting at a few dollars per month, online markets for DDoS attacks (so-called *booters* or *stressers*) allow unskilled actors to flood online services with unwanted traffic, knocking systems without robust security offline [5]. Booter operators may justify their services as testing server resilience, but their primary uses and methods are illegal [6].

The entrepreneurial, service-based nature of booters makes them vulnerable to targeted interventions. Although individual arrests may be generally ineffective in industrialised market crime economies as they aid competitors, the economic forces driving these markets tend to lead to the centralisation of the infrastructure and supportive work on which they depend (through well-understood efficiencies and network externalities). Booter infrastructure consolidation therefore presents an apposite target for disruption activities. In a major takedown event in December 2018, 15 of the largest booters were seized in an international law enforcement effort [7]. However, the effect was relatively short-lived, with DDoS attack volumes recovering a few weeks later [8, 9].

Building on practitioner learning and academic analysis of previous efforts, a further major intervention was conducted from late 2022, combining targeting infrastructure with influence operation components: 49 booter domains were seized in December 2022 (the first wave) [10], 13 domains were seized in May 2023 (the second wave) [11], and several deceptive sites were set up by law enforcement. This campaign has been much greater in scale and more persistent than the one four years earlier, leading us to ask: how effective might it be?

There are several material aspects of online crime that make

UNIVERSITY OF CAMBRIDGE · THE UNIVERSITY of EDINBURGH · University of Strathclyde Glasgow · UIC UNIVERSITY OF ILLINOIS CHICAGO

Anh V. Vu — anh.vu@cst.cam.ac.uk