

# Cybercrime in a Shopping Cart

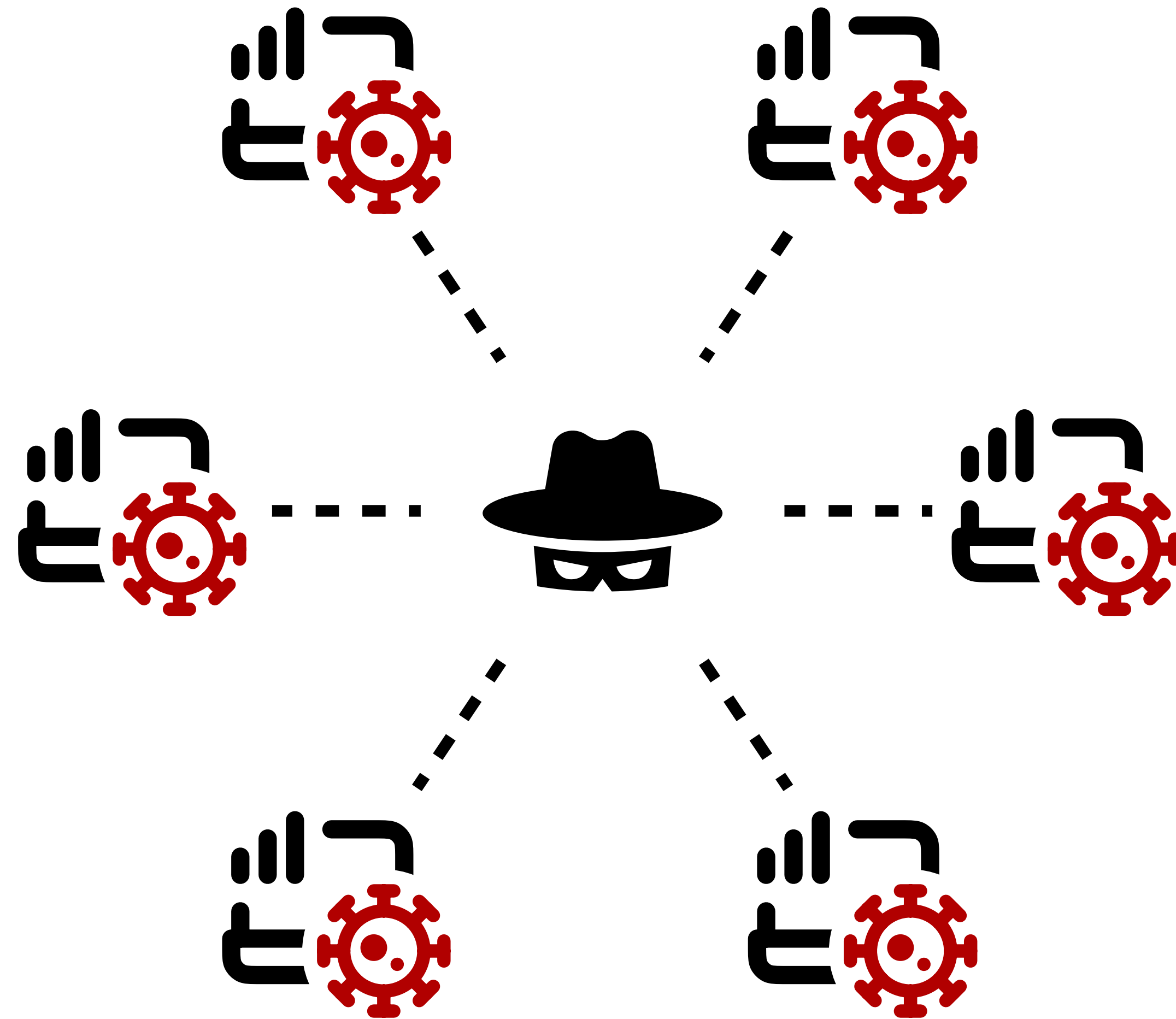
Investigating the DDoS-for-Hire ecosystem

Maarten Weyns

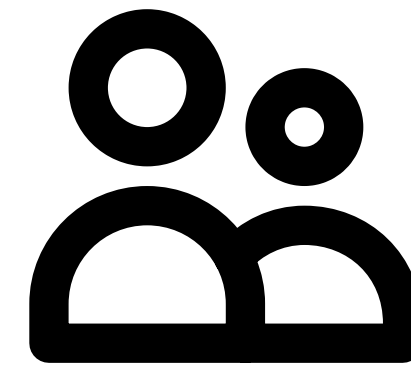
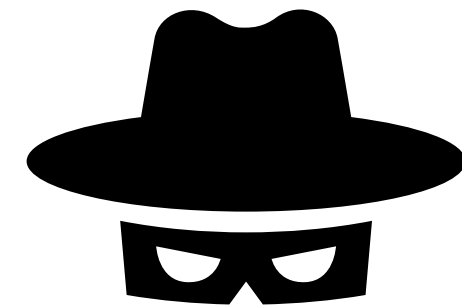


**DDoS-for-Hire**

# DDoS-for-Hire





# DDoS-for-Hire






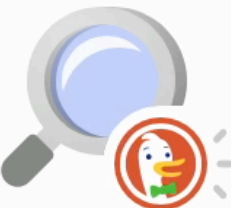
# DDoS-for-Hire

 DuckDuckGo

 Duck.ai




## Switch to DuckDuckGo. It's private and free!



Make DuckDuckGo your default search engine.

Set As Default Search

BEST PRIVACY



Get our free browser for even more privacy.

Download Browser →


Trusted by tens of millions worldwide!

Learn more

# DDoS-for-Hire

nightmare-stresser.com  
silentstress.net  
zerostress.st  
redstresser.net  
diamstress.ru  
webdown.su  
netdowner.su  
mao-stress.su  
elitestress.st  
stresscat.ru  
stresser.ba  
anarchystress.su  
darkvr.ru  
vacstresser.ru  
stressers.su  
nbyte.pw  
dumpcord.cc  
vire.cc  
sattelitestresser.st  
fluxstress.to  
goliathstress.st  
stresslab.st  
silencestresser.ru  
rebirthstress.net  
vipstresser.net

# DDoS-for-Hire




[Dashboard](#)

## Feel The **True Charms** Of DDoS.

Use **FLUXSTRESS** to test the protection of your website, server or network against real DDoS attacks.


[Explore More](#)



## FLUXSTRESS

### Your **#1** stress testing service

Get ahead with **Fluxstress** stress testing - avoid downtime and keep your website and services performing at their best.



No login logs, attack logs cleared weekly.



# Of DDoS.

Use **FLUXSTRESS** to test the protection of your website, server or network against real DDoS attacks.

Explore More

## FLUXSTRESS Your #1 stress testing service

Get ahead with **Fluxstress** stress testing - avoid downtime and keep your website and services performing at their best.



No login logs, attack logs cleared weekly.



Method can bypass OVH, Cloudflare and more protections.



Easy to use attack panel

## Features



### Safe & Secure

We do not save login logs, we delete attack logs every week.



### Cheap Plans

We have very cheap plans + very strong power



### Discounts

We often give discount codes on our telegram

## Features



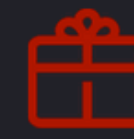
### Safe & Secure

We do not save login logs, we delete attack logs every week.



### Cheap Plans

We have very cheap plans + very strong power



### Discounts

We often give discount codes on our telegram

## EXCLUSIVE Services We Offer



### Payments

Anonymous and instant payments allow you to order our services whenever you want.



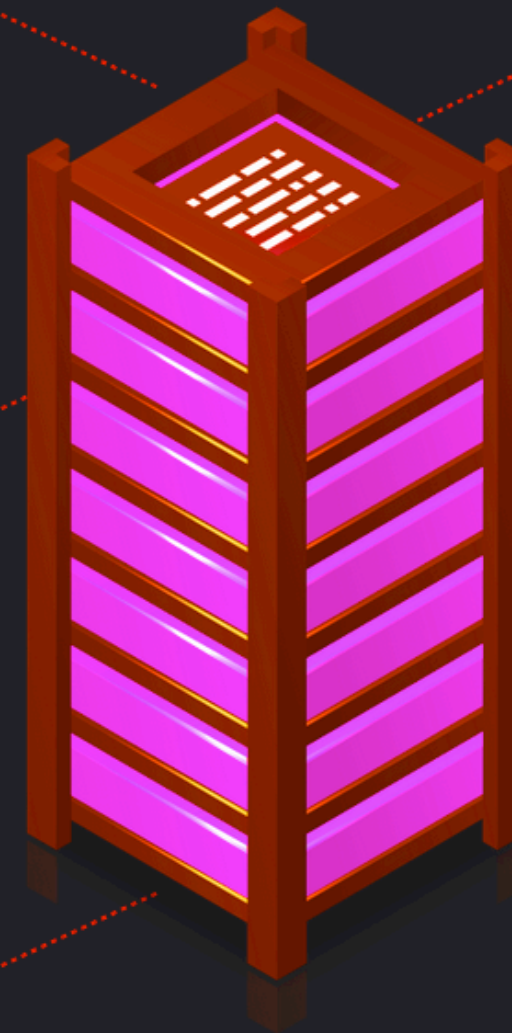
### Advanced methods

With our self-coded solution and usage of high-quality proxies, we are currently providing the best bypasses and power stability on the market. Keep in mind that it won't work on all targets.



### Cheap Plans

We try the best to keep our prices as low and fair as possible.



### Support

Our support replies within 24 hours, we always will help you with every problem you face



### Uptime

We provide a high power uptime, and we compensate any downtime.



### Easy control panel

Slick UI panel that will let you simulate stress tests against your server/website/IP. We have an amazing panel, easy-to-use.

Dashboard

53 User online

lucosia  
elw94s87veiruy@proton.me

Dashboard

Stress Panel

Purchase

Deposit

API Manager

Support

TOTAL USERS  
60457

TOTAL ATTACKS  
2095320

RUNNING ATTACKS  
74

PAID USERS  
312

News

Top Methods

TLS-VIP (27%)

543685

CLOUDFLARE (17%)

347826

BROWSER (8%)

161082

TLS-SPAM (8%)

157638

NTP (7%)

130778

CLDAP (5%)

109125

TLS-FREE (4%)

88532

TCP-SYN (3%)

66504

UDPBYPASS (3%)

59754

We now offer a limited-time 5% discount! Use coupon code FREE5 at checkout.

DarkVR

Home

Attack Panel

Buy Plan

API Manager

Support

Attack Methods

Telegram Support

User pogstresser

Users  
44,224

Servers Usage (L7)  
11%

Servers Usage (L4)  
18%

Total Methods  
26

News

New Telegram/Signal Contacts 12 days ago

Our previous telegram contacts has been deleted, we have created a new telegram contacts.

To find our new telegram/signal contacts: <https://darkvr.ru/support.html> (signal coming soon)

Currently Working Domains 4 months ago

Our previous domains a

Currently Working Ba

darkvr.ru

Big Update: Layer-7 Me

We've been working har

now they're more power

Membership Plan

Buy Me

You don't h

Buy now to e

We Do Not U

We Have S

vs vire.cc

Network Stress Testing

MAIN

Dashboard

Purchase

HUB

Attack Manager

Welcome back, ppsgod

Here's what's happening with vire.cc today.

32  
Online users

Online  
Support status

473,263  
Total proxies

279  
Ongoing attacks

Profile

Username: ppsgod

Plan: none

Boot Time: 0(s)

Concurrents: 0

Balance: \$0

Goliath Services

Main

Dashboard

Attacks

Documentation

Billing

Plans

Deposit

Dashboard

Total Users  
1,156  
More than yesterday ↗  
Users for the whole time

Total Attacks  
34,014  
More than yesterday ↗  
Attacks for the whole time

Running Attacks  
405  
Used out of 1,250 slots  
Attacks that are currently running


Announcements  
News and updates of the project.

Information  
Summary of your current plan.

Plan Free

Concurrents 0 attacks





Dashboard

Stress Panel

Purchase

Deposit

API Manager

Support

TOS

Telegram

PowerProof

Community

Reviews / Feedback

Contact Team

Stress Panel

39 User online

Lucosia

elw94s87veiruy@proton.me

Stress Panel

Layer 4

Layer 7

Host

1.1.1.1

Port

80

Time

60

Attack Method

UDP-FREE

Concurrents

1

Send Attack

Running Attacks

STOP ALL

Show 10 entries

ID

Target

Method

Expire

Action

No running attacks! :(

Showing 0 to 0 of 0 entries

<<>>

Proxy Statistics (Last 15min)

Global

22845

Germany

4304

United States

3028

United Kingdom

2220

France

2118

China

1427

Thailand

1231

Indonesia

1088

Canada

1076

Spain

1045

Italy

1037

Brazil

705

South Korea

288

Singapore

253

Philippines

249

Hong Kong SAR China

225

Bangladesh

193

India

190

Japan

153

Colombia

148

Netherlands

141

Russia

125

United Arab Emirates

119

Vietnam

99

Mexico

95

Türkiye

93

Others

1195

12

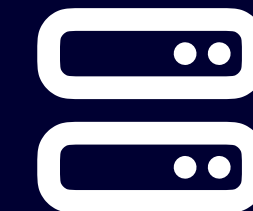
## Layer 4

|                     |           |
|---------------------|-----------|
| NTP amplification   | TCP       |
| TCP amplification   | TCPBYPASS |
| CLDAP amplification | TCP-OVH   |
| WSD amplification   | TCP-SYN   |
| DNS amplification   | HOME      |
| UDP bypass          | GAME      |
| UDP OVH             | ICMP      |
| SYNACK              | FIVEM     |
| VSE                 | FORTNITE  |
| TCP-ACK             | DISCORD   |

## Layer 7

|          |                   |
|----------|-------------------|
| TLS-SPAM | Cloudflare bypass |
| TLS-VIP  | Browser bypass    |
| COOKIE   |                   |


# Concurrents





# Concurrents





Dashboard

Stress Panel

Purchase

Deposit

API Manager

Support

TOS

Telegram

PowerProof

Community

Reviews / Feedback

Contact Team

≡

Purchase

53 User online

lucosia

elw94s87veiruy@proton.me

Basic-01

\$35.00/month

2 concurrent

300 seconds

Premium

API access

Prioritized support

Purchase

Basic-02

\$70.00/month

4 concurrent

600 seconds

Premium

API access

Prioritized support

Purchase

Basic-03

\$140.00/month

8 concurrent

1200 seconds

Premium

API access

Prioritized support

Purchase

Basic-04

\$200.00/month

12 concurrent

1200 seconds

Premium

API access

Prioritized support

Purchase

September-Sale-01

\$195.00/month

15 concurrent

900 seconds

Premium

API access

Prioritized support

Purchase

September-Sale-02

\$245.00/month

20 concurrent

1200 seconds

Premium

API access

Prioritized support

Purchase

September-Sale-03

\$290.00/month

25 concurrent

1200 seconds

Premium

API access

Prioritized support

Purchase

September-Sale-04

\$335.00/month

30 concurrent

1500 seconds

Premium

API access

Prioritized support

Purchase

Premium-01

\$150.00/month

8 concurrent

600 seconds

Premium

API access

Prioritized support

Premium-02

\$280.00/month

16 concurrent

1200 seconds

Premium

API access

Prioritized support

Premium-03

\$430.00/month

24 concurrent

3000 seconds

Premium

API access

Prioritized support

Premium-04

\$530.00/month

30 concurrent

3600 seconds

Premium

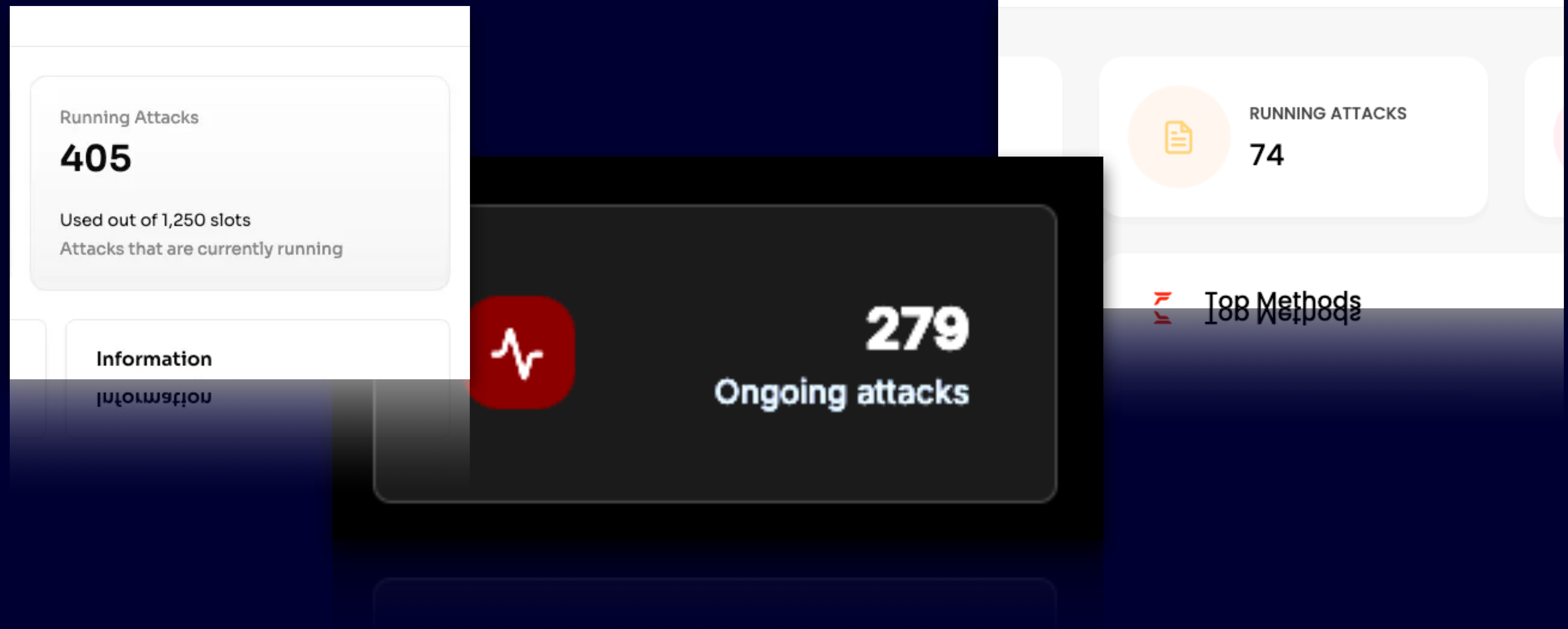
API access

Prioritized support

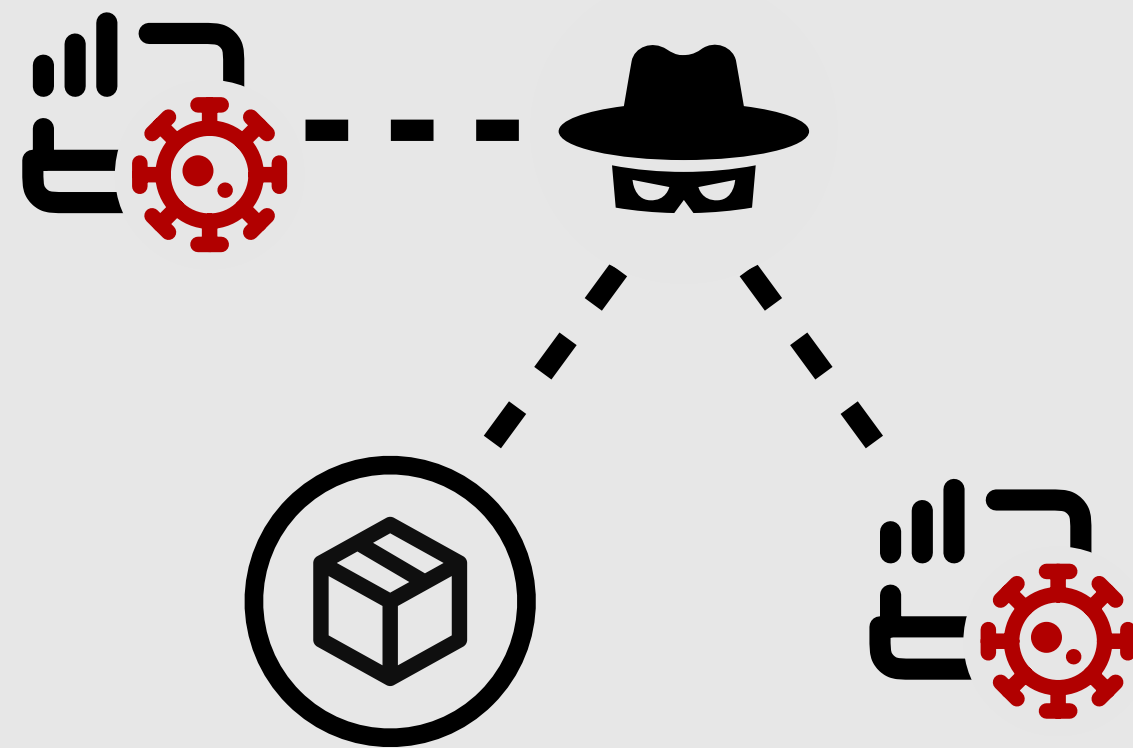
# Measuring a DDoS Botnet



# Measuring a DDoS Botnet

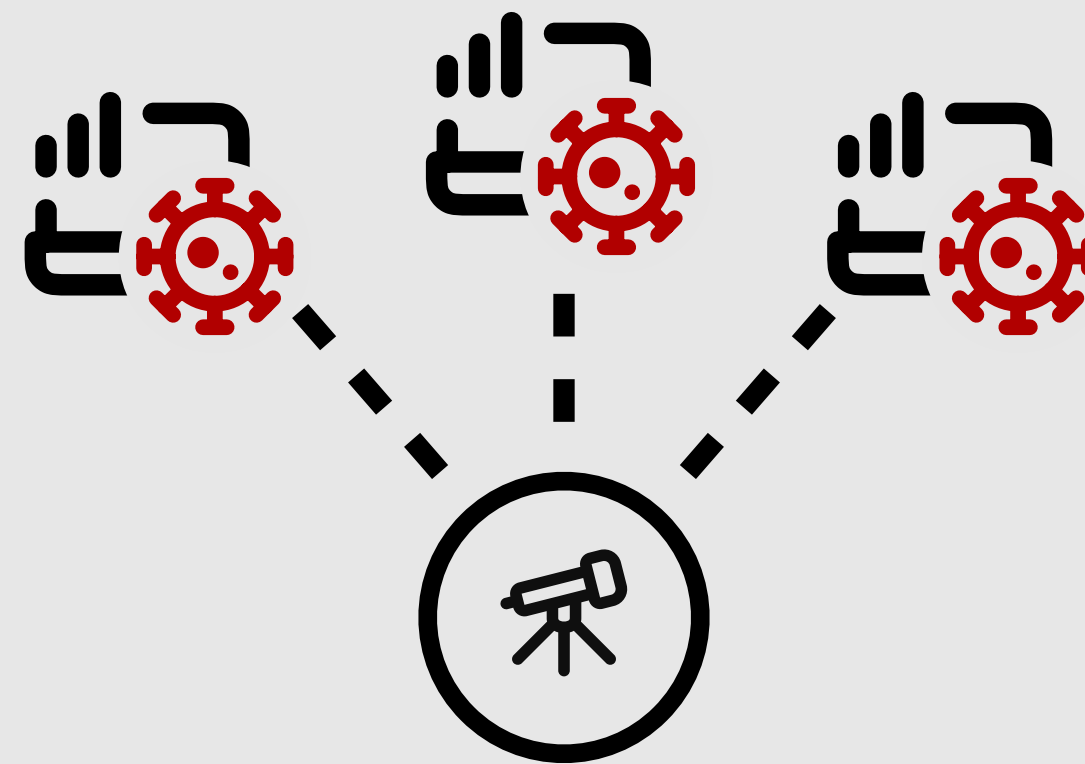


# Measuring a DDoS Botnet



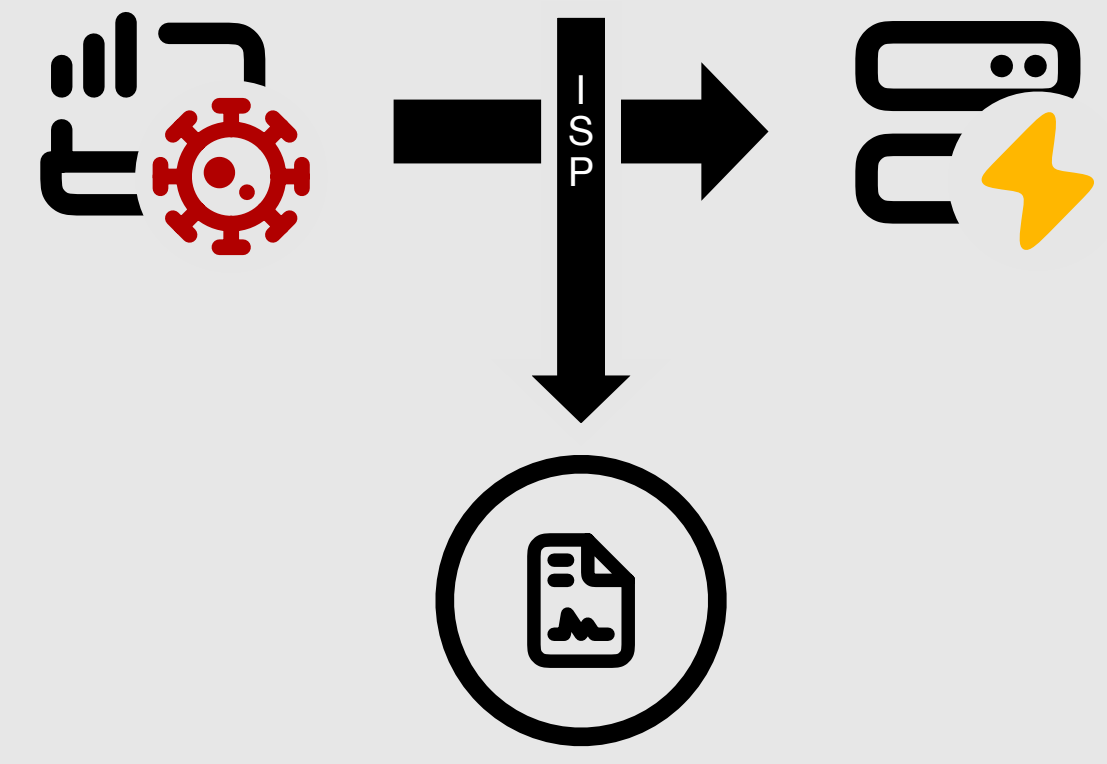
How many attacks  
are conducted?

Simulate infection  
and join the network



How many bots  
are in the network?

Sensors collecting  
scanning traffic



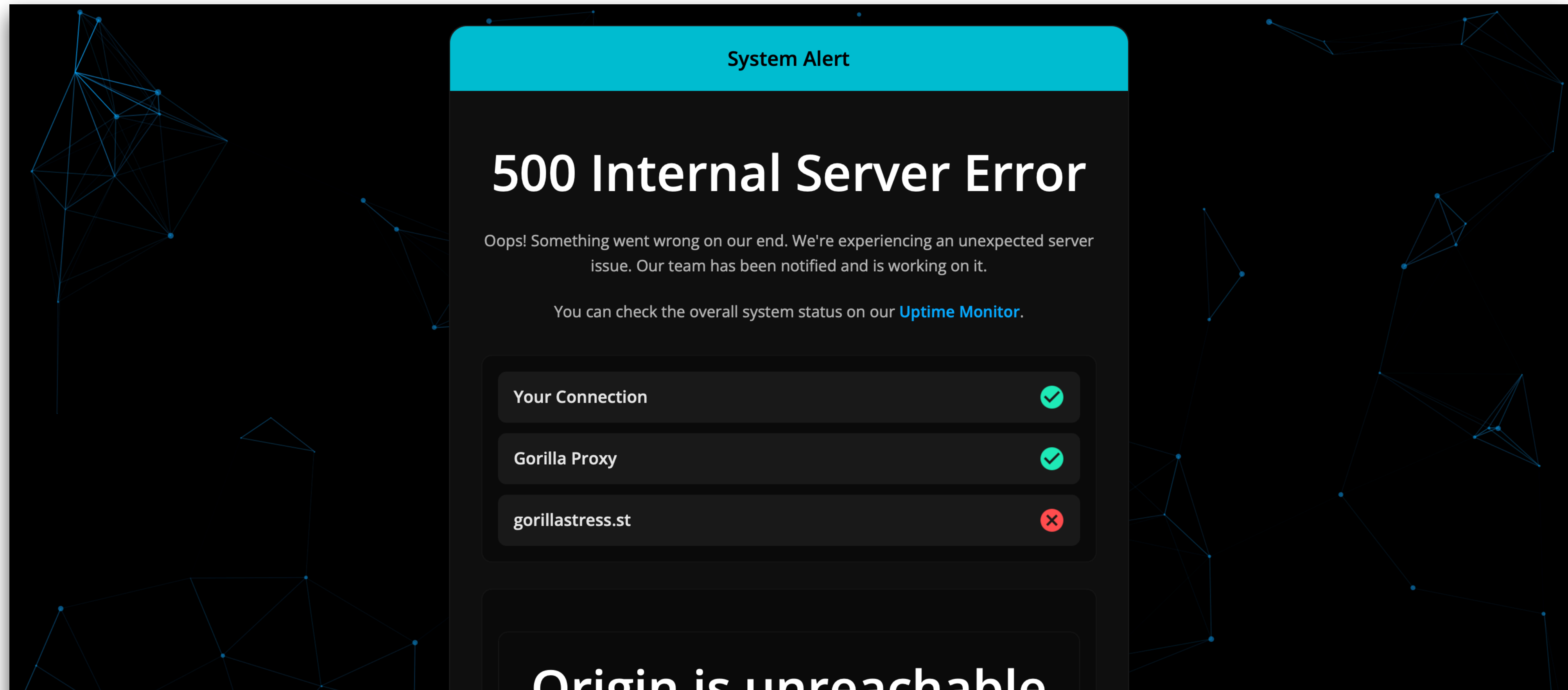
How large are  
attacks?

Netflow data from  
Internet Service Providers

# Gorilla Stresser

# Gorilla Stresser

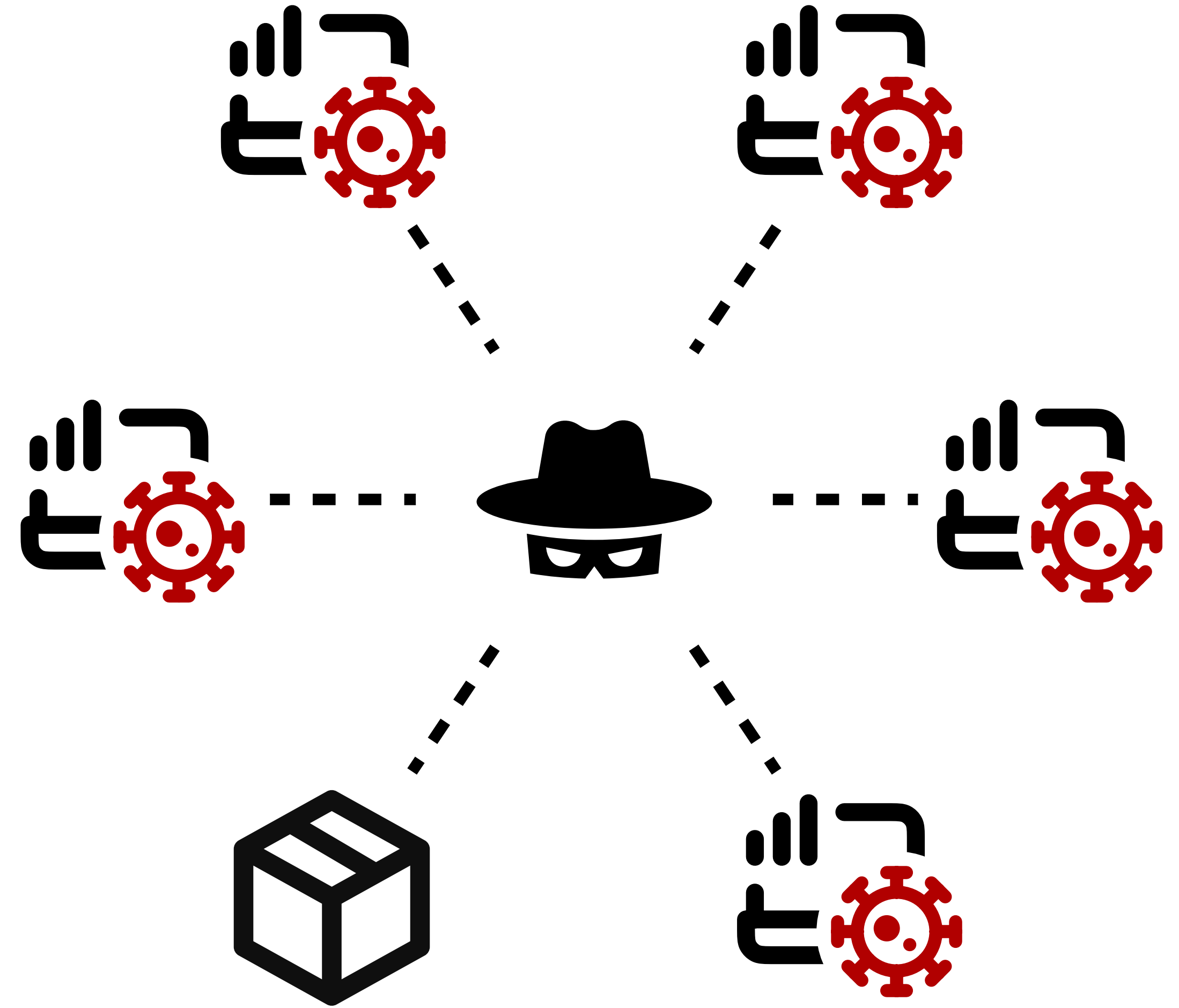
- Observed in detail between September 2024 and June 2025





# Gorilla Stresser

- Simulate a Gorilla Botnet infection
  - Observe all commands in the network



**740 351**

Attacks

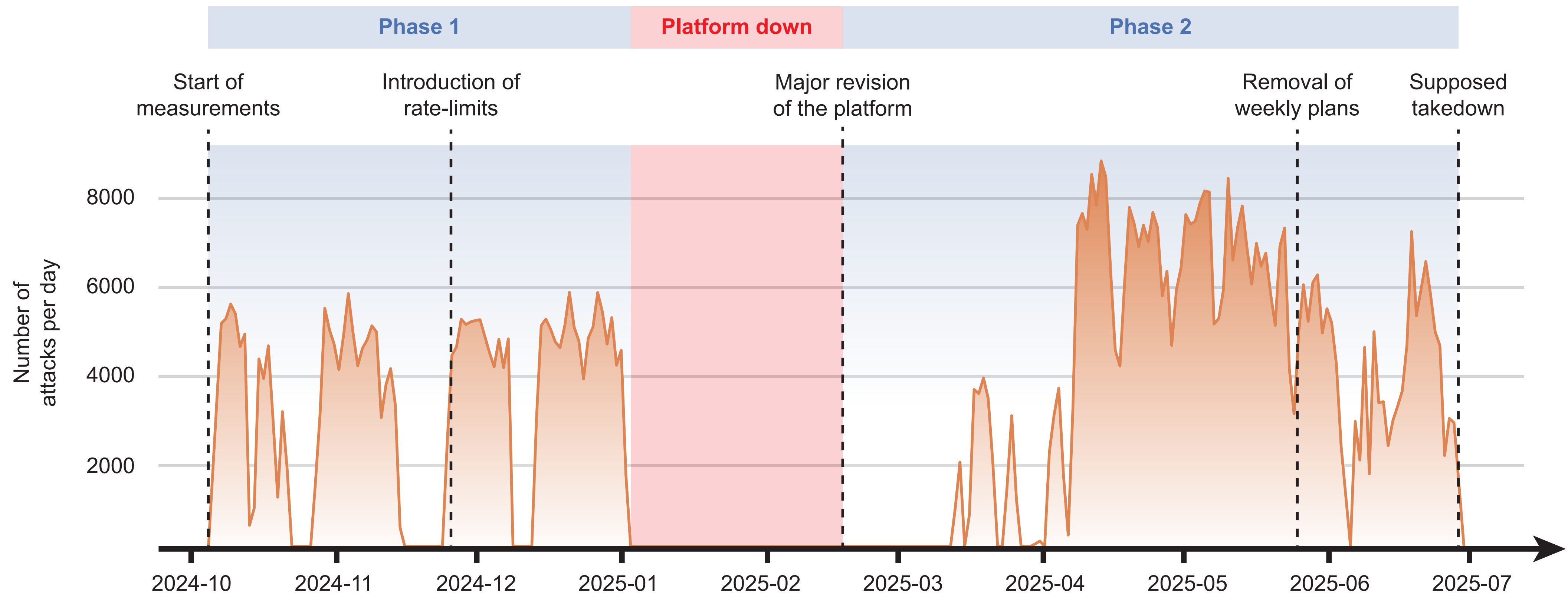
**146 213**

Unique victims

**4 596**

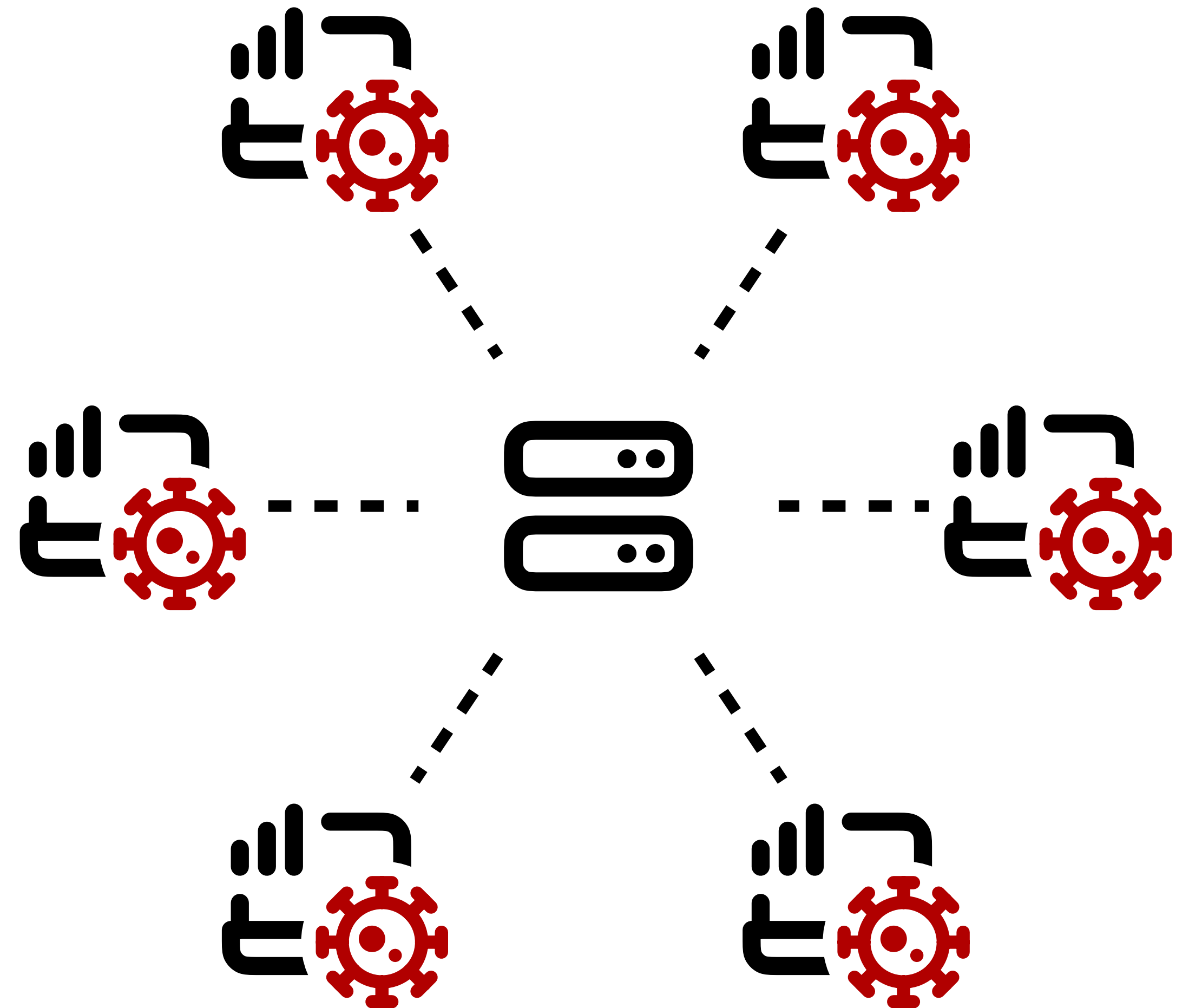
Attacks / day

# Gorilla Stresser



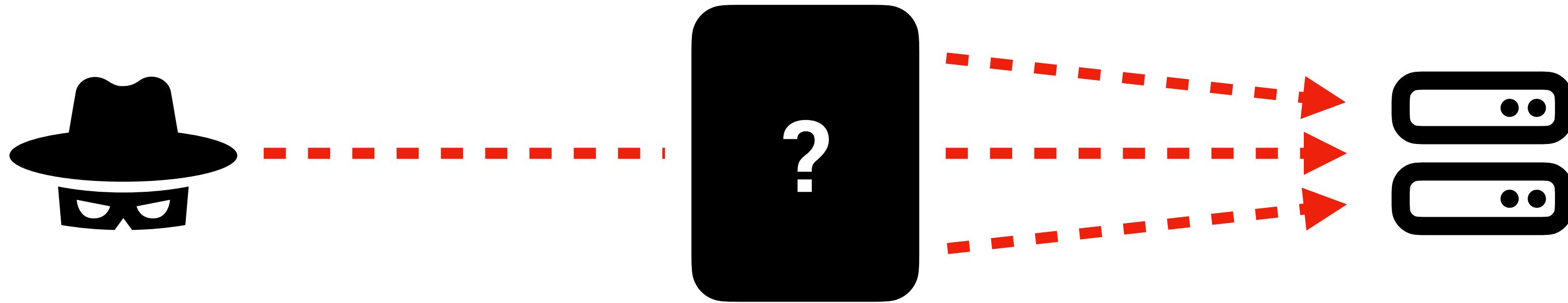
# Gorilla Stresser

- Disposable botnet
  - Only a single hard-coded C2 server



# Life after botnets

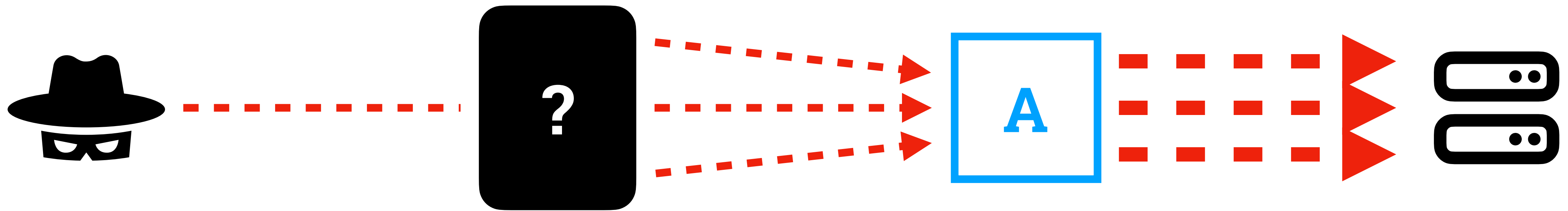
- Using centralised infrastructure



- Easier to maintain...
  - ... and allows for spoofed traffic! 🤯

# Life after botnets

- Allows for reflection and amplification attacks

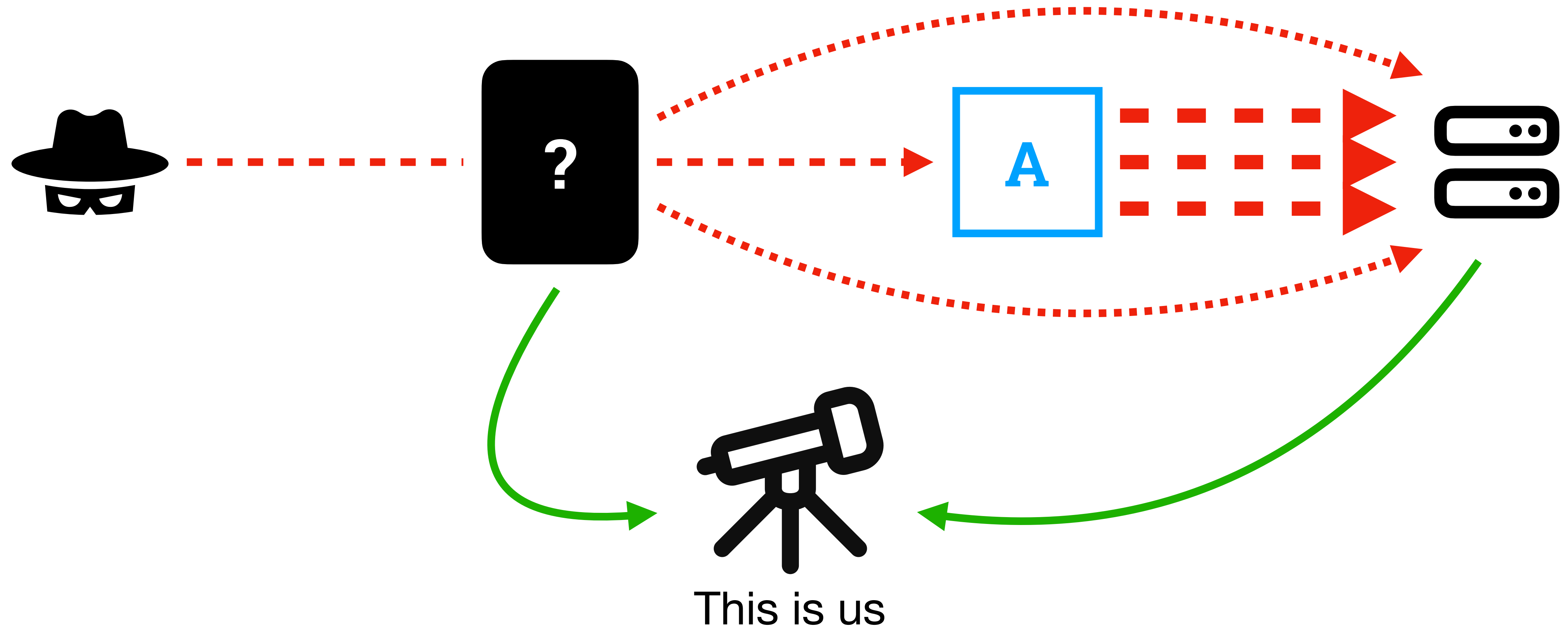


- Becomes more difficult to track...
  - ...but not impossible!



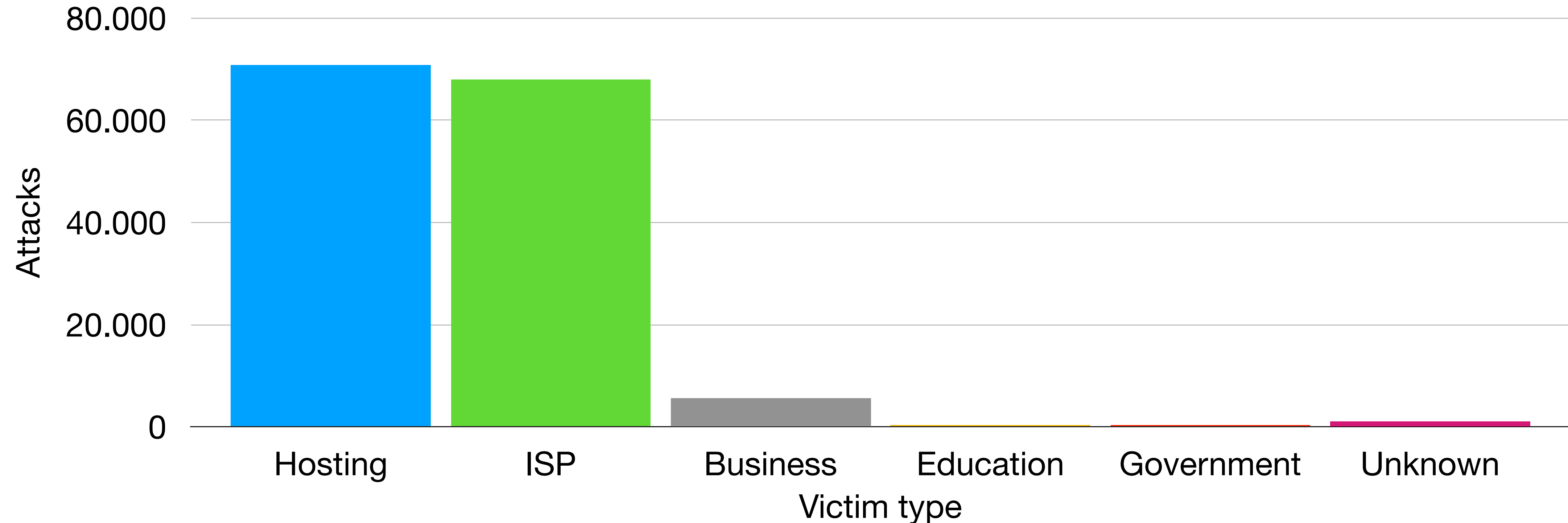
# Life after botnets

- Observing noise from the attack



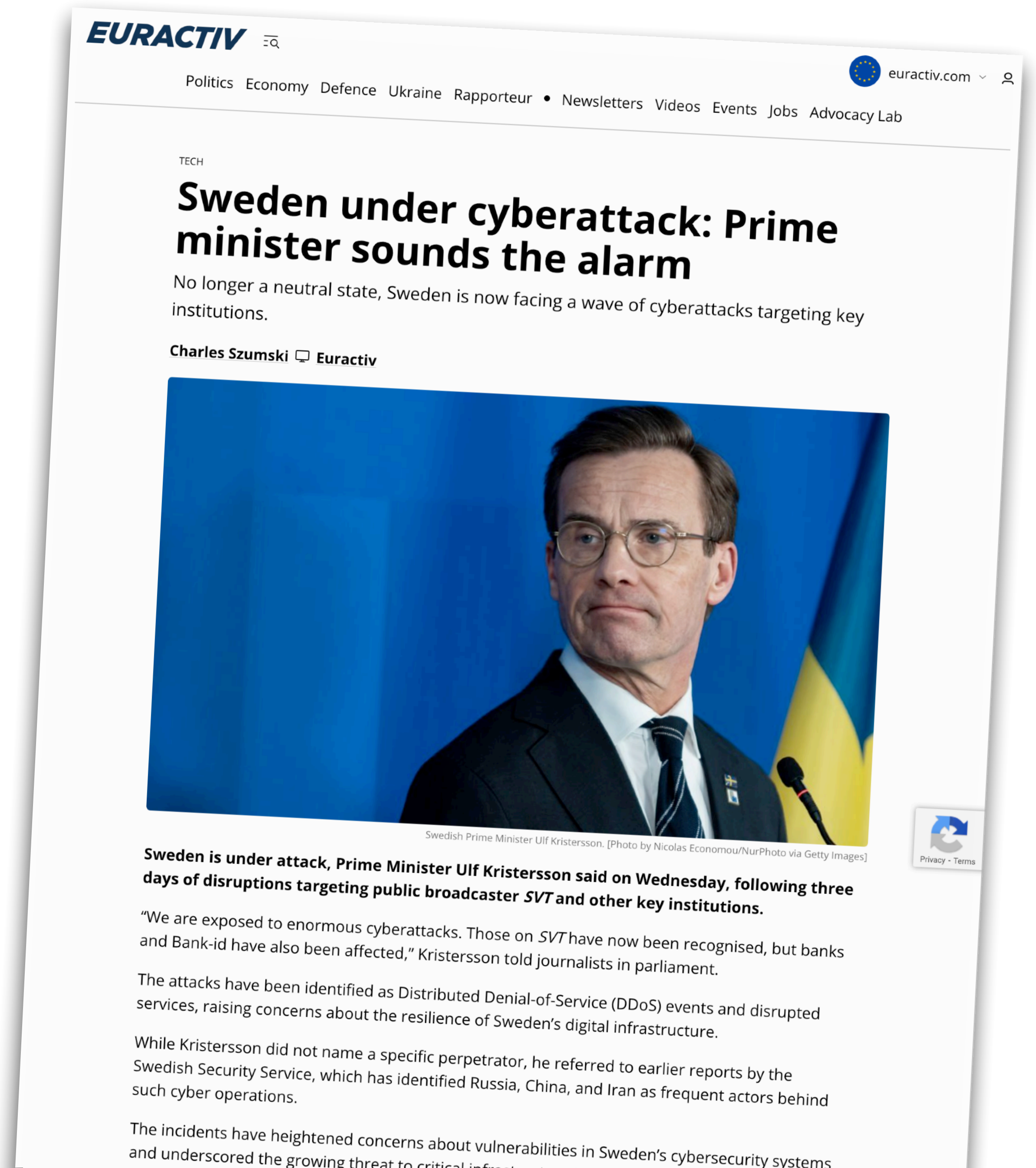
# Gorilla Stresser

- Mainly hosting providers and home internet connections targeted



# Gorilla Stresser

- Attributed attacks
  - Swedish broadcasting service (SVT)





# Go

- Att



Swedish Prime Minister Ulf Kristersson. [Photo by Nicolas Economou/NurPhoto via Getty Images]



[Privacy](#) - [Terms](#)

**Sweden is under attack, Prime Minister Ulf Kristersson said on Wednesday, following three days of disruptions targeting public broadcaster *SVT* and other key institutions.**

“We are exposed to enormous cyberattacks. Those on *SVT* have now been recognised, but banks and Bank-id have also been affected,” Kristersson told journalists in parliament.

The attacks have been identified as **Distributed Denial-of-Service (DDoS) events** and disrupted services, raising concerns about the resilience of Sweden’s digital infrastructure.

While Kristersson did not name a specific perpetrator, he referred to earlier reports by the Swedish Security Service, which has identified Russia, China, and Iran as frequent actors behind such cyber operations.

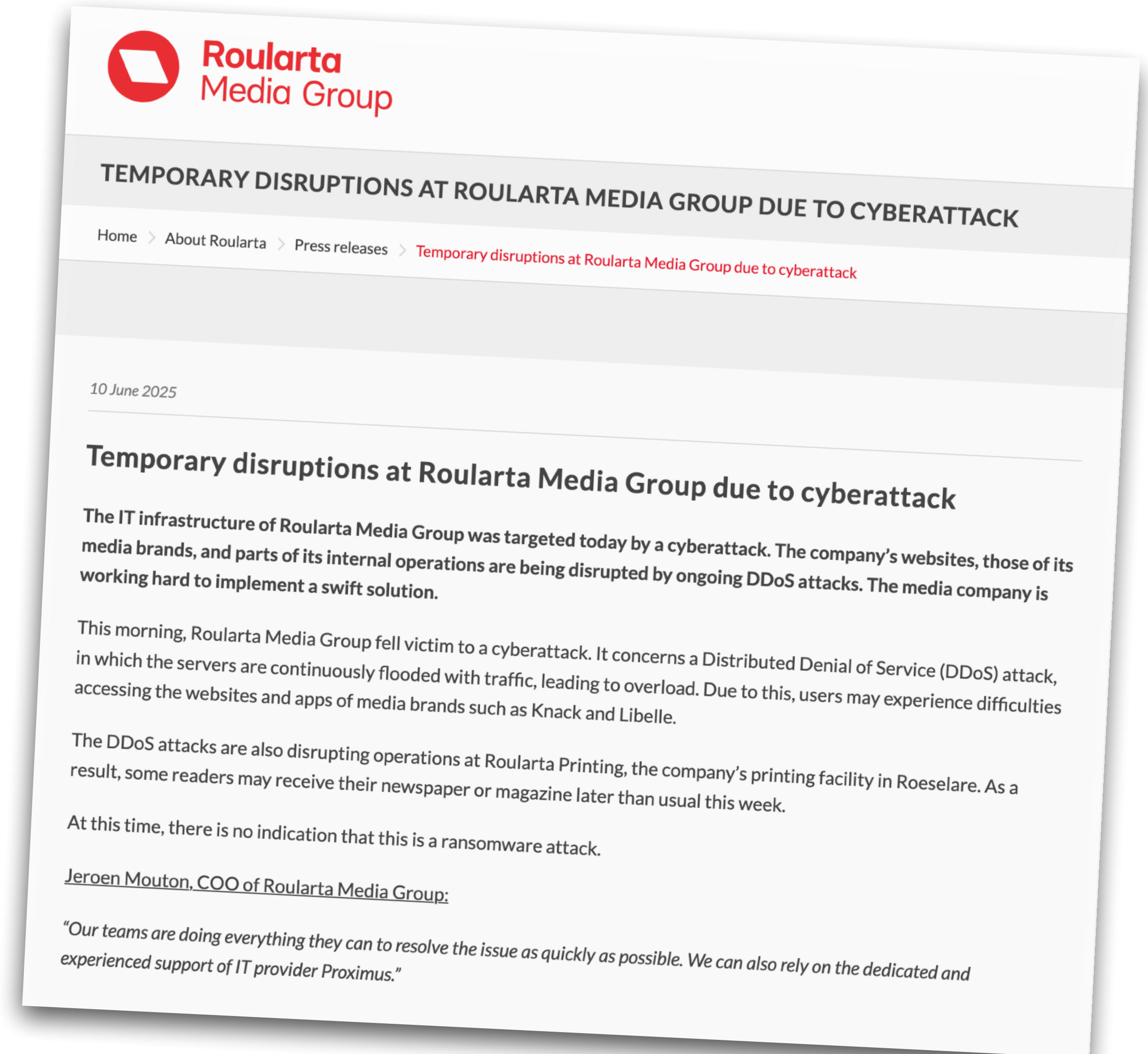
The incidents have heightened concerns about vulnerabilities in Sweden’s cybersecurity systems and underscored the growing threat to critical infrastructure in one of the world’s most connected nations, where over **93% of households** have internet access.

Cybersecurity experts have warned that such breaches could escalate, impacting not just digital services, but also public trust.

The attacks come amid heightened geopolitical tensions. Sweden’s recent accession to NATO and its support for Ukraine have likely made it a more prominent target for cyberattacks, including

# Gorilla Stresser

- Attributed attacks
  - Swedish broadcasting service (SVT)
  - Roularta Media Group





# Gorilla

- Attribute
- Swe
- (SV
- Rou

10 June 2025

## Temporary disruptions at Roularta Media Group due to cyberattack

The IT infrastructure of Roularta Media Group was targeted today by a cyberattack. The company's websites, those of its media brands, and parts of its internal operations are being disrupted by ongoing DDoS attacks. The media company is working hard to implement a swift solution.

This morning, Roularta Media Group fell victim to a cyberattack. It concerns a Distributed Denial of Service (DDoS) attack, in which the servers are continuously flooded with traffic, leading to overload. Due to this, users may experience difficulties accessing the websites and apps of media brands such as Knack and Libelle.

The DDoS attacks are also disrupting operations at Roularta Printing, the company's printing facility in Roeselare. As a result, some readers may receive their newspaper or magazine later than usual this week.

At this time, there is no indication that this is a ransomware attack.

Jeroen Mouton, COO of Roularta Media Group:

*"Our teams are doing everything they can to resolve the issue as quickly as possible. We can also rely on the dedicated and experienced support of IT provider Proximus."*



# Gorilla Stresser

nightmare-stresser.com

silentstress.net

zerostress.st

redstresser.net

diamstress.ru

webdown.su

netdowner.su

elitestress.st

mao-stress.su

stresscat.ru

stresser.ba

darkvr.ru

stressers.su

anarchystress.su

vacstresser.ru

nbyte.pw

dumpcord.cc

vire.cc

sattelitestresser.st

fluxstress.to

goliathstress.st

stresslab.st

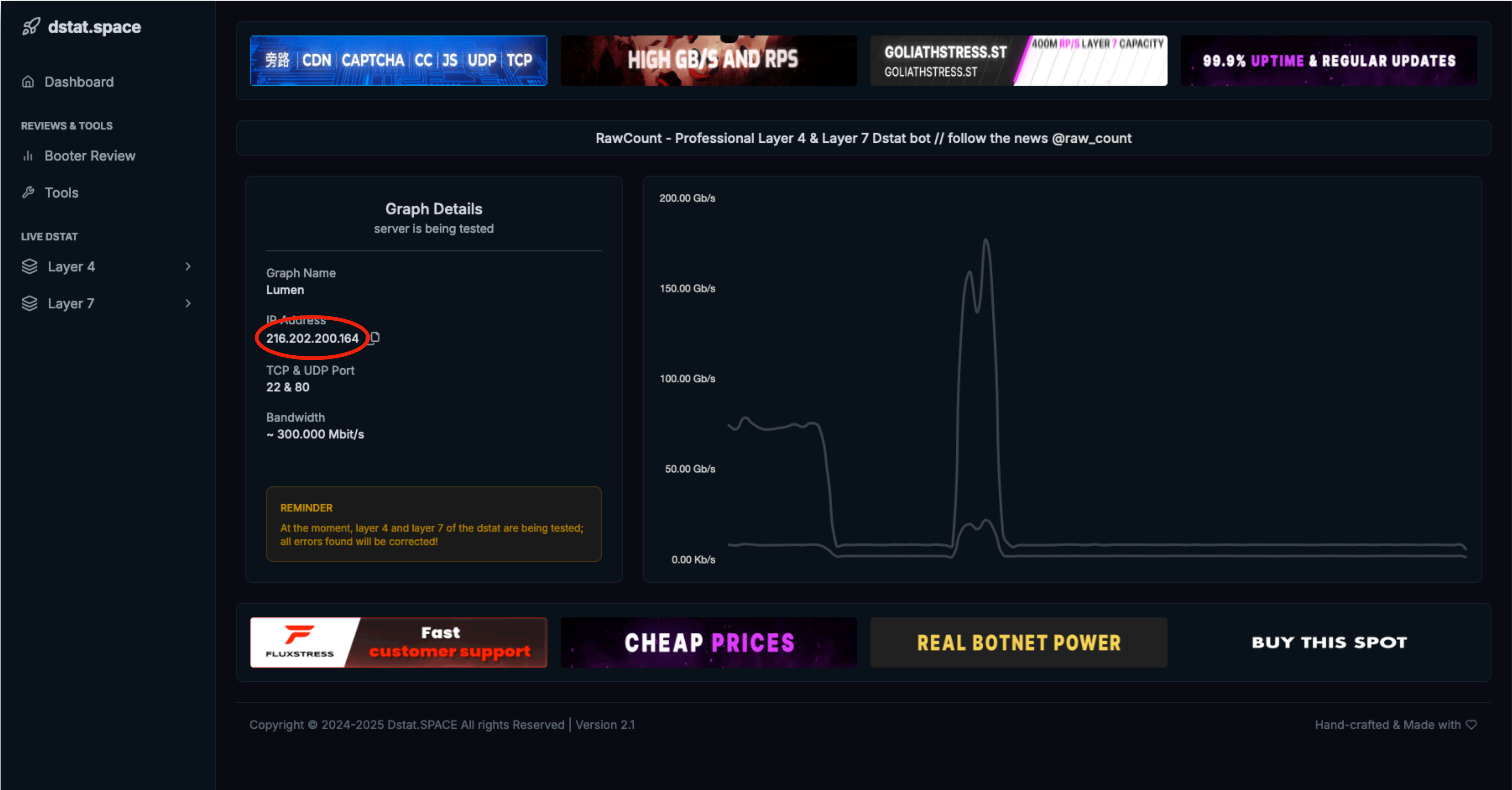
silencestresser.ru

rebirthstress.net

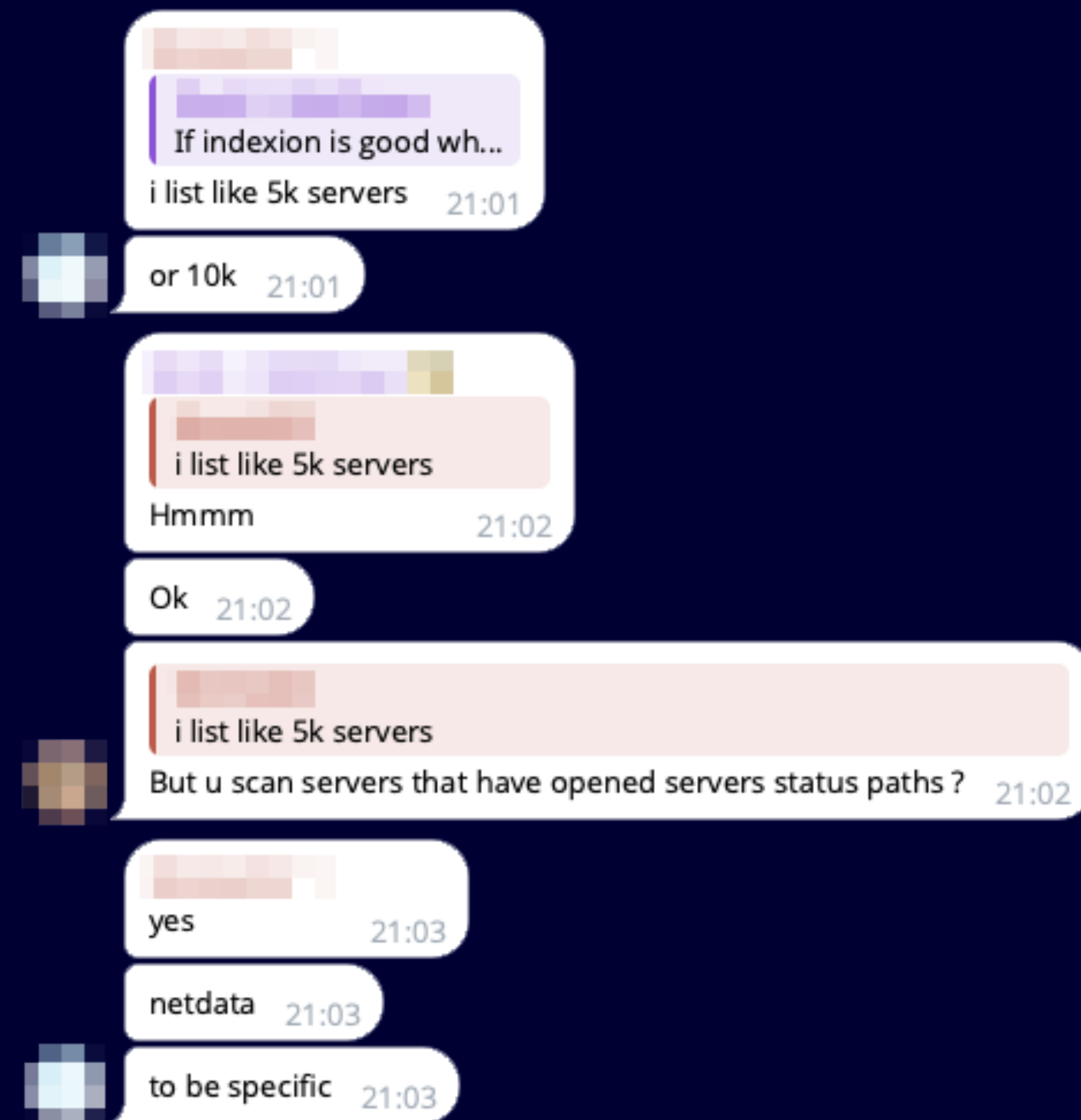
vipstresser.net

**Enabling the market**

# Enabling the market



# Enabling the market



netdata 21:03

to be specific 21:03

bro

01:15

canada is full ← 2 01:15

of netdatas 01:15

```
.9999 (Netdata v2.8.0-10-nightly) - 10.00 Gbps
.9999 (Netdata v1.33.1) - 1.00 Gbps
ind: 36847523 1.48 Mp/s (1.47 Mp/s avg); recv: 8835 348 p/s (352 p/s)
.10000 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 25.00 Gbps
.9999 (Netdata v2.6.1) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.0-10-nightly) - 10.00 Gbps
ind: 38325479 1.48 Mp/s (1.47 Mp/s avg); recv: 9189 353 p/s (352 p/s)
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v1.46.0-103-nightly) - 10.00 Gbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.10000 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v1.47.0) - 1.00 Gbps
.9999 (Netdata v1.30.1-135-nightly) - 100.00 Mbps
.10000 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.0-2-nightly) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 25.00 Gbps
ind: 39804066 1.48 Mp/s (1.47 Mp/s avg); recv: 9539 349 p/s (352 p/s)
.9999 (Netdata v1.33.1) - 25.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v1.44.3) - 2.50 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v1.33.1) - 1.00 Gbps
.9999 (Netdata v2.8.0-10-nightly) - 1.00 Gbps
.9999 (Netdata v1.35.0-26-gbadcabc) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 10.00 Gbps
.10000 (Netdata v2.8.1) - 100.00 Gbps
.9999 (Netdata v1.43.0-284-nightly) - 10.00 Gbps
.10000 (Netdata v2.7.3) - 100.00 Gbps
ind: 41270445 1.47 Mp/s (1.47 Mp/s avg); recv: 9886 346 p/s (352 p/s)
.9999 (Netdata v2.6.0-13-nightly) - 1.00 Gbps
.9999 (Netdata v1.19.0-381-nightly) - 1.00 Mbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.0-10-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
ind: 42745722 1.47 Mp/s (1.47 Mp/s avg); recv: 10270 392 p/s (353 p/s)
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 10.00 Gbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.10000 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.10000 (Netdata v2.8.1) - 100.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.10000 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v1.21.1-28-nightly) - 1.00 Mbps
.9999 (Netdata v2.7.3) - 1.00 Gbps
.9999 (Netdata v2.5.0-292-nightly) - 25.00 Gbps
.9999 (Netdata reboot-16540-g52bfc4ef5d) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
ind: 44222603 1.48 Mp/s (1.47 Mp/s avg); recv: 10614 334 p/s (353 p/s)
.9999 (Netdata v2.7.0-237-nightly) - 25.00 Gbps
```



```
ind: 36847523 1.48 Mp/s (1.47 Mp/s avg); rcv: 8835 348 p/s (352 p/s)
.9999 (Netdata v1.33.1) - 1.00 Gbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 25.00 Gbps
.9999 (Netdata v2.6.1) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.0-10-nightly) - 10.00 Gbps
ind: 38325479 1.48 Mp/s (1.47 Mp/s avg); rcv: 9189 353 p/s (352 p/s)
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v1.46.0-103-nightly) - 10.00 Gbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v1.47.0) - 1.00 Gbps
.9999 (Netdata v1.30.1-135-nightly) - 100.00 Mbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.0-2-nightly) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 25.00 Gbps
ind: 39804066 1.48 Mp/s (1.47 Mp/s avg); rcv: 9539 349 p/s (352 p/s)
.9999 (Netdata v1.33.1) - 25.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v1.44.3) - 2.50 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v1.33.1) - 1.00 Gbps
.9999 (Netdata v2.8.0-10-nightly) - 1.00 Gbps
.9999 (Netdata v1.35.0-26-gbadcabc) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 10.00 Gbps
.9999 (Netdata v2.8.1) - 100.00 Gbps
.9999 (Netdata v1.43.0-204-nightly) - 10.00 Gbps
.9999 (Netdata v2.7.3) - 100.00 Gbps
ind: 41270445 1.47 Mp/s (1.47 Mp/s avg); rcv: 9886 346 p/s (352 p/s)
.9999 (Netdata v2.6.0-13-nightly) - 1.00 Gbps
.9999 (Netdata v1.19.0-381-nightly) - 1.00 Mbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.0-10-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
ind: 42745722 1.47 Mp/s (1.47 Mp/s avg); rcv: 10270 392 p/s (353 p/s)
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.7.0-237-nightly) - 10.00 Gbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v1.33.1-28-nightly) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 100.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
.9999 (Netdata v2.8.1) - 1.00 Gbps
.9999 (Netdata v1.21.1-28-nightly) - 1.00 Mbps
.9999 (Netdata v2.7.3) - 1.00 Gbps
.9999 (Netdata v2.5.0-292-nightly) - 25.00 Gbps
.9999 (Netdata reboot-16540-g52bfc4ef5d) - 1.00 Gbps
.9999 (Netdata v2.8.1) - 10.00 Gbps
ind: 44222603 1.48 Mp/s (1.47 Mp/s avg); rcv: 10614 334 p/s (353 p/s)
.9999 (Netdata v2.7.0-237-nightly) - 25.00 Gbps
```

send me one ill make dstat 01:16

[http://\[redacted\]:19999/](http://[redacted]:19999/) ← 2 01:17

100g 01:17

non protected im pretty sure ← 1 01:17

copy

|       |                  |   |        |      |
|-------|------------------|---|--------|------|
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.8.1) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |
| 19999 | (Netdata v2.7.3) | - | 100.00 | Gbps |

← 3 01:18

i got a few 01:18



[illegible]

## Results

Report Docs

## Host Filters

## Labels:

36.06K google-tag-manager  
34.21K remote-access  
9,139 proxy  
7,656 email  
6,397 database  
[More](#)

## Autonomous System:

4,178 KIXS-AS-KR Korea Telecom  
4,058 HETZNER-AS  
3,853 OVH  
3,419 NESSUS  
2,551 ASDETUK  
www.heficed.com  
[More](#)

## Location:

6,326 South Korea  
5,640 United States  
4,951 Germany  
4,546 United Kingdom  
4,368 France  
[More](#)

## Service Filters

## Service Names:

184.07K HTTP  
36.57K SSH  
25.24K PORTMAP  
17.23K SMTP  
11.39K UNKNOWN  
[More](#)

## Hosts

Results: 45,174 Time: 0.13s

## 185.245.228.88 (nwt5.mailcampaign.de)

Hpe Ilo NESSUS (47692) Vienna, Austria

email google-tag-manager out-of-band-management network-administration

25/SMTP 110/POP3 161/SNMP 587/SMTP 995/POP3  
2049/PORTMAP 2301/HTTP 2381/HTTP 8081/HTTP 19999/HTTP  
39342/PORTMAP 45126/PORTMAP 49659/PORTMAP 56915/PORTMAP

## 83.137.112.10 (news5.swiss-ad.com)

Hpe Ilo NESSUS (47692) Vienna, Austria

out-of-band-management google-tag-manager network-administration email

25/SMTP 110/POP3 161/SNMP 587/SMTP 995/POP3  
2049/PORTMAP 2301/HTTP 2381/HTTP 8081/HTTP 19999/HTTP  
39342/PORTMAP 45126/PORTMAP 49659/PORTMAP 56915/PORTMAP

## 108.170.13.142

Linux SSASN2 (20454) Arizona, United States

web.control-panel.hosting file-sharing email login-page database

25/SMTP 53/DNS 80/HTTP 110/POP3 111/PORTMAP  
111/PORTMAP 143/IMAP 443/HTTP 465/SMTP 587/SMTP  
993/IMAP 995/POP3 2078/UNKNOWN 2082/HTTP 2083/HTTP  
2086/HTTP 2087/HTTP 2095/HTTP 2096/HTTP 3306/MYSQL  
9824/FTP 19999/HTTP

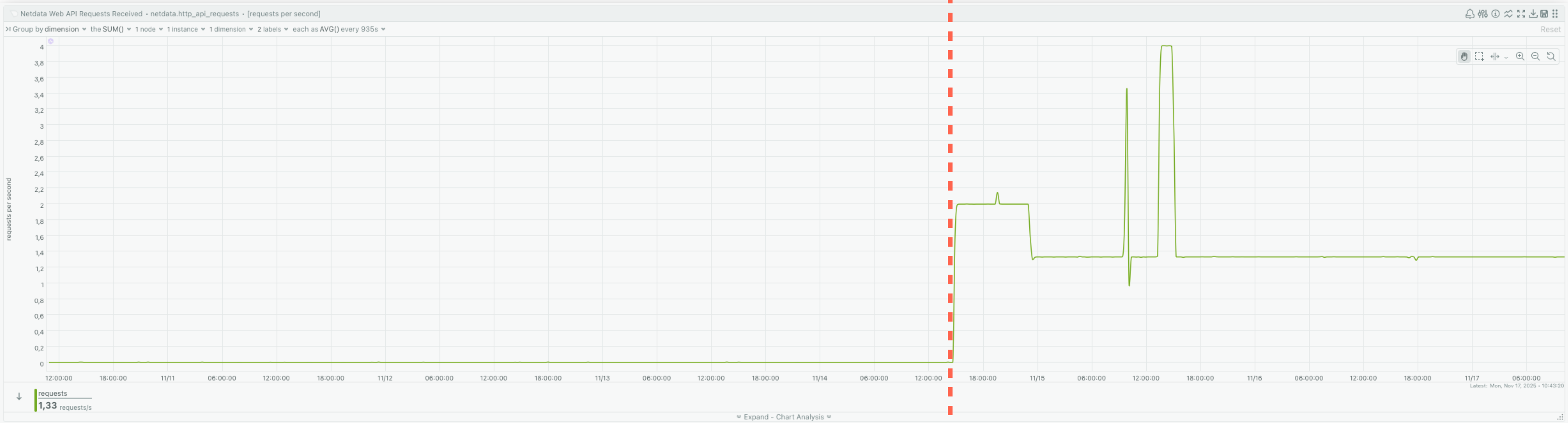
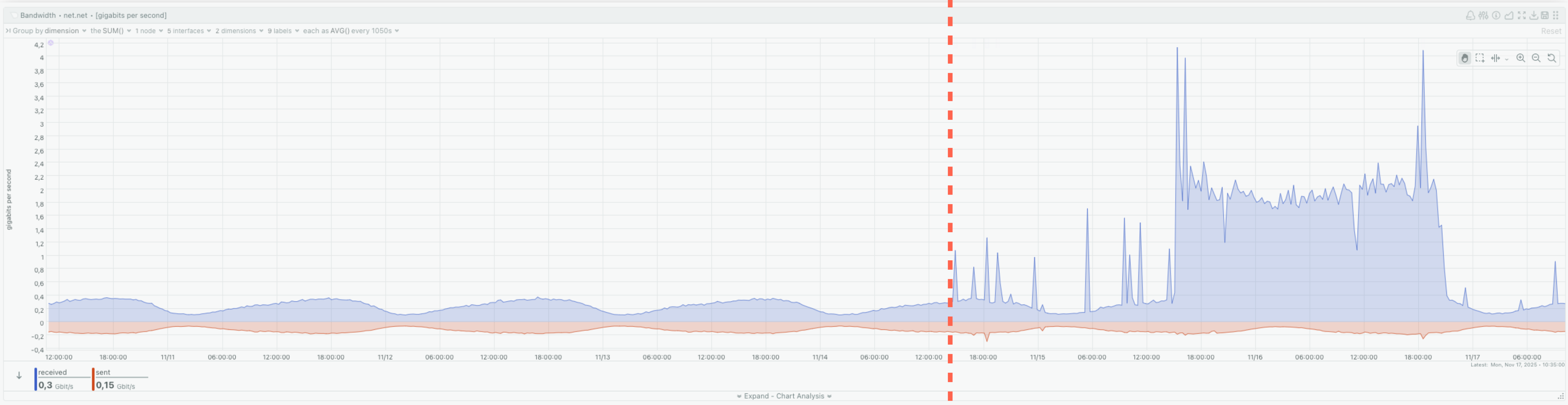
## 78.157.34.172

Linux DADE-SAMANE-FANAVA www.Fanavaidc.com (62442) Tehran, Iran

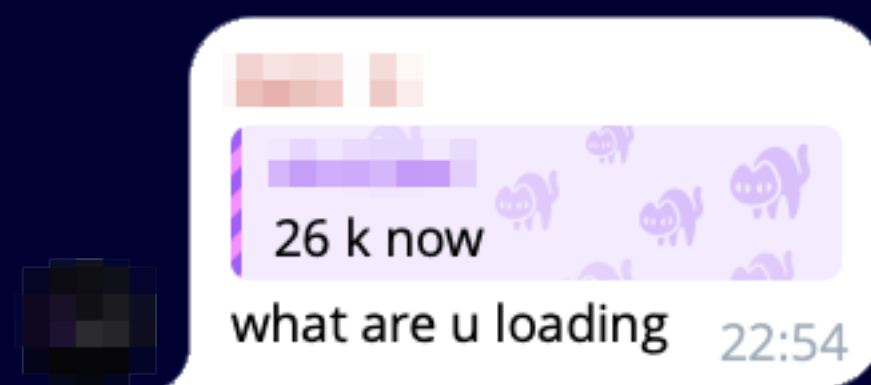
google-tag-manager network.device.vpn remote-access




22/SSH 80/HTTP 443/HTTP 500/IKE 992/HTTP  
1193/HTTP 1194/HTTP 1194/OPENVPN 5555/HTTP 19999/HTTP


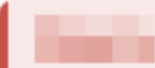
## 51.83.55.226 (ip226.ip-51-83-55.eu)

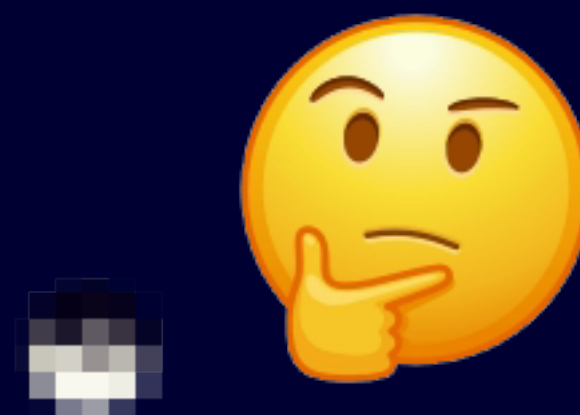



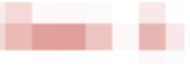



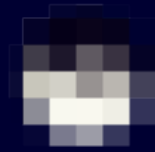



   
 26 k now  
what are u loading 22:54

  
 what are u loading  
cameras 22:54



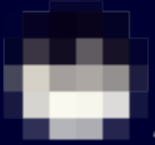
   
 cameras  
oh 22:54



  
 cameras  
oh 22:54


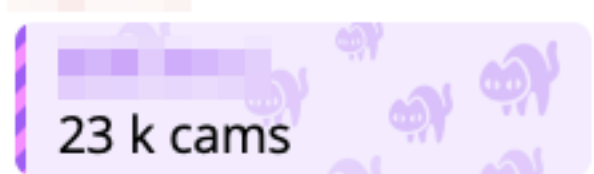
  
23 k cams ← 2 22:54

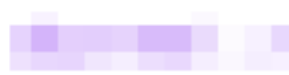

1k router 22:54



2 k fridge I think 22:55



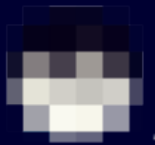
  
 23 k cams  
whats the output 22:55

  
  
whats the output  
2tbit on the cams by themselves 22:55

and around 3 with all devices 22:55

I mean we started last night dude 22:55

wait untill the end of the month 22:55



and we proolly will have 1 mil ← 4 22:56

maybe 200k u can depen...

kinda limited by money 22:56

As of rn I'm spending 30usd per day ← 4 22:56

Not much 22:57

But 22:57

It adds up 22:57

As of rn I'm spending ...

could be worse 22:57

Reply

could be worse

yea 22:57

yea

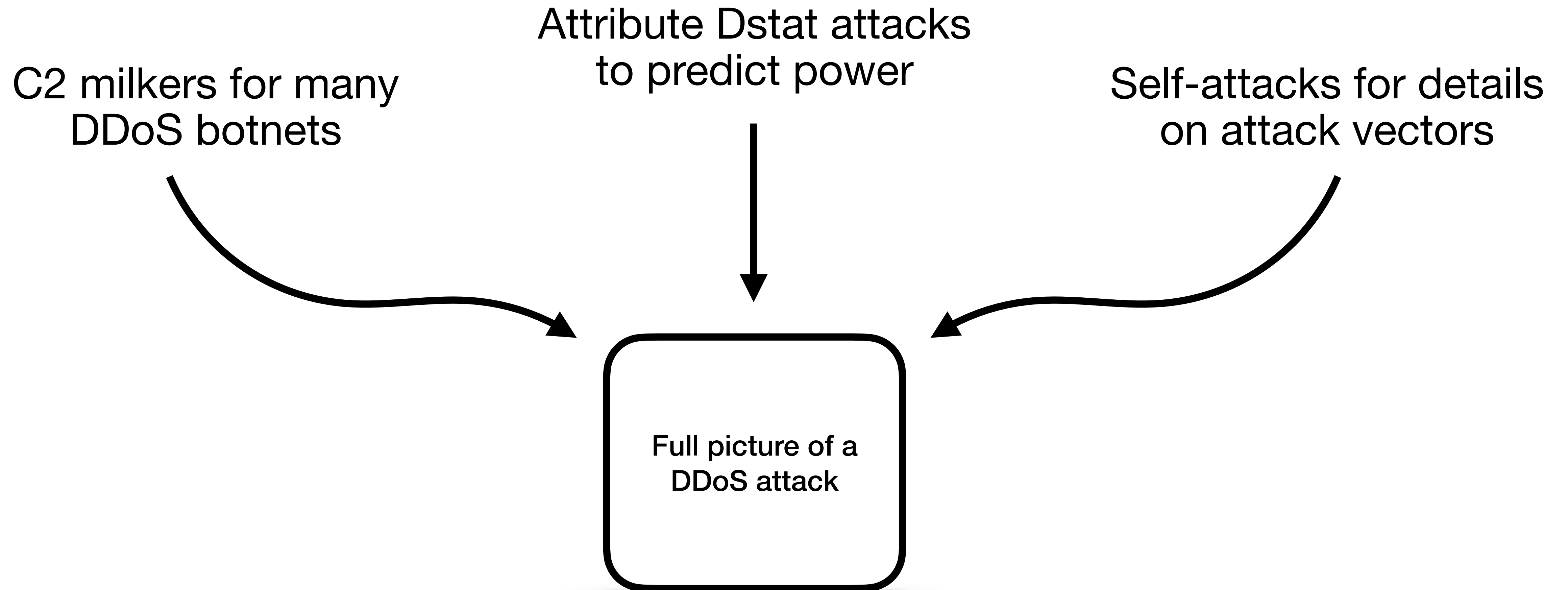
just abuse serveroffer 22:57

we loaded like 40k bots 22:57

just with their servers ← 3 22:57

**The next steps**

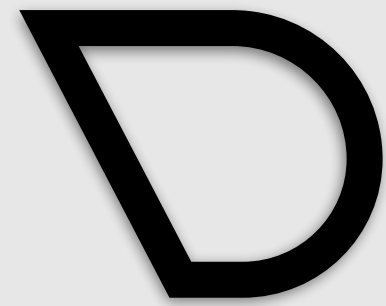
# The next steps





**We might need some help**

# We might need some help



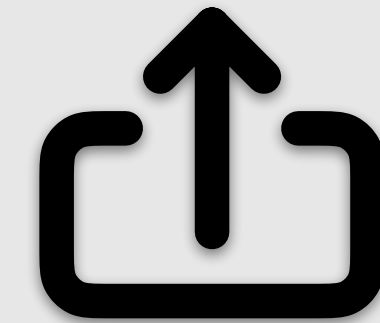
## Netdata honeypots

Gather intelligence on  
DDoS test attacks



## Self-attacks

Get information on  
attack vectors

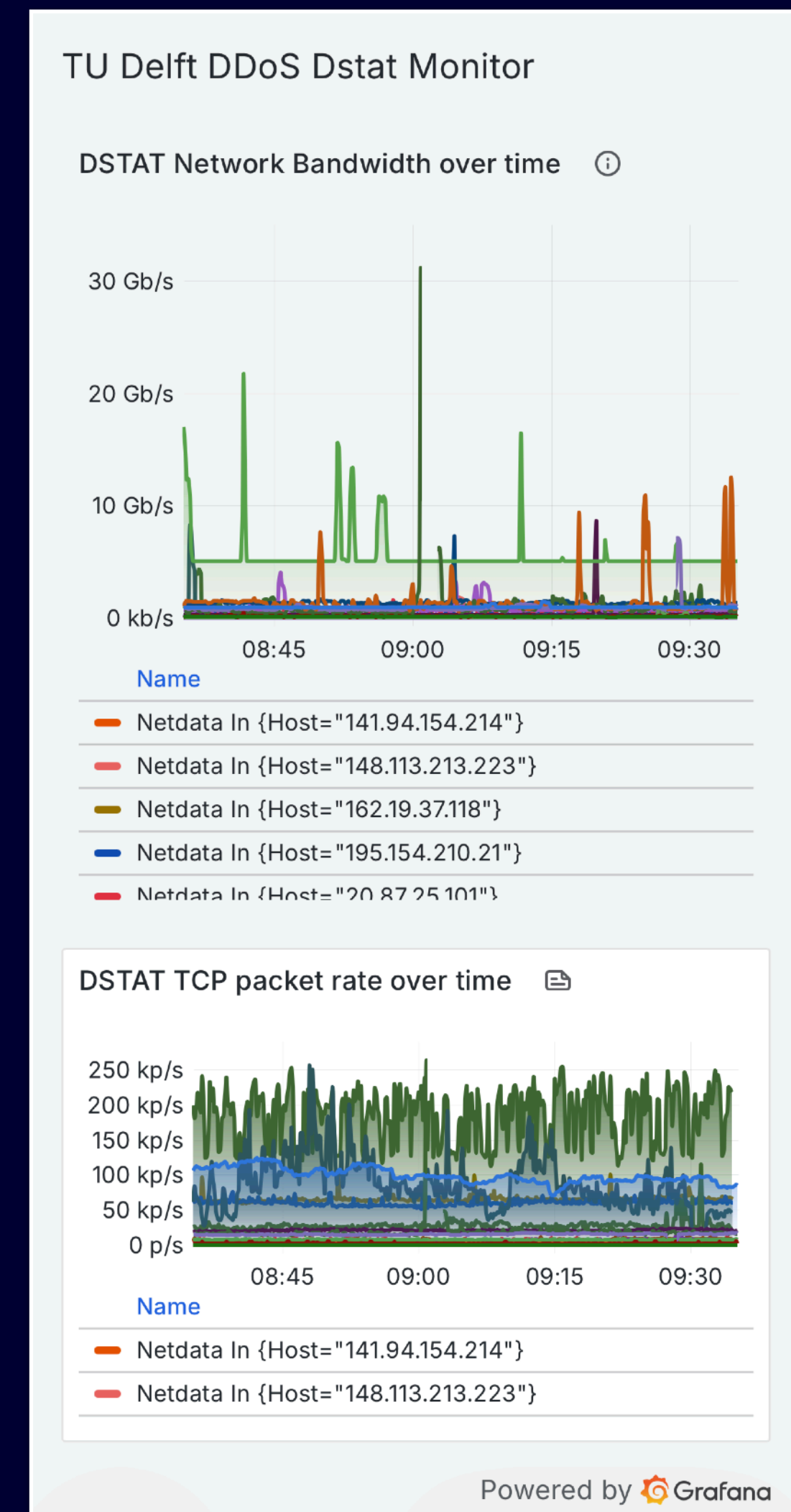


## Data sharing

Attribution, intelligence,  
technical details, ...

# View our dashboard

- Live traffic from monitored Dstat endpoints





# Cybercrime in a Shopping Cart

Investigating the DDoS-for-Hire ecosystem

Maarten Weyns