Microplastics of the Internet

Finding and Fighting Hidden Attack Traffic

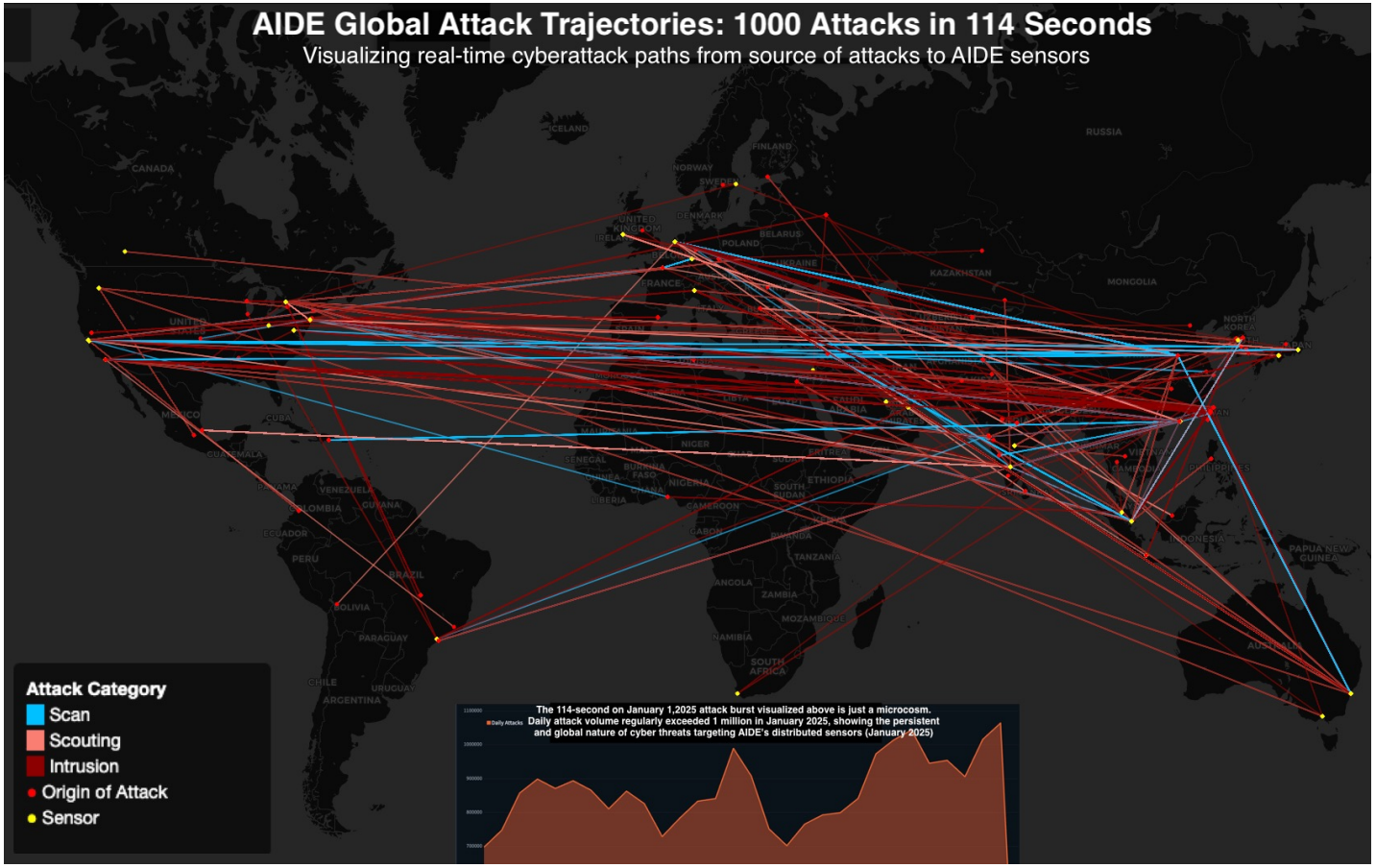
LESLIE DAIGLE, GLOBAL CYBER ALLIANCE

RIPE 90


ATTACKS BY THE
NUMBERS

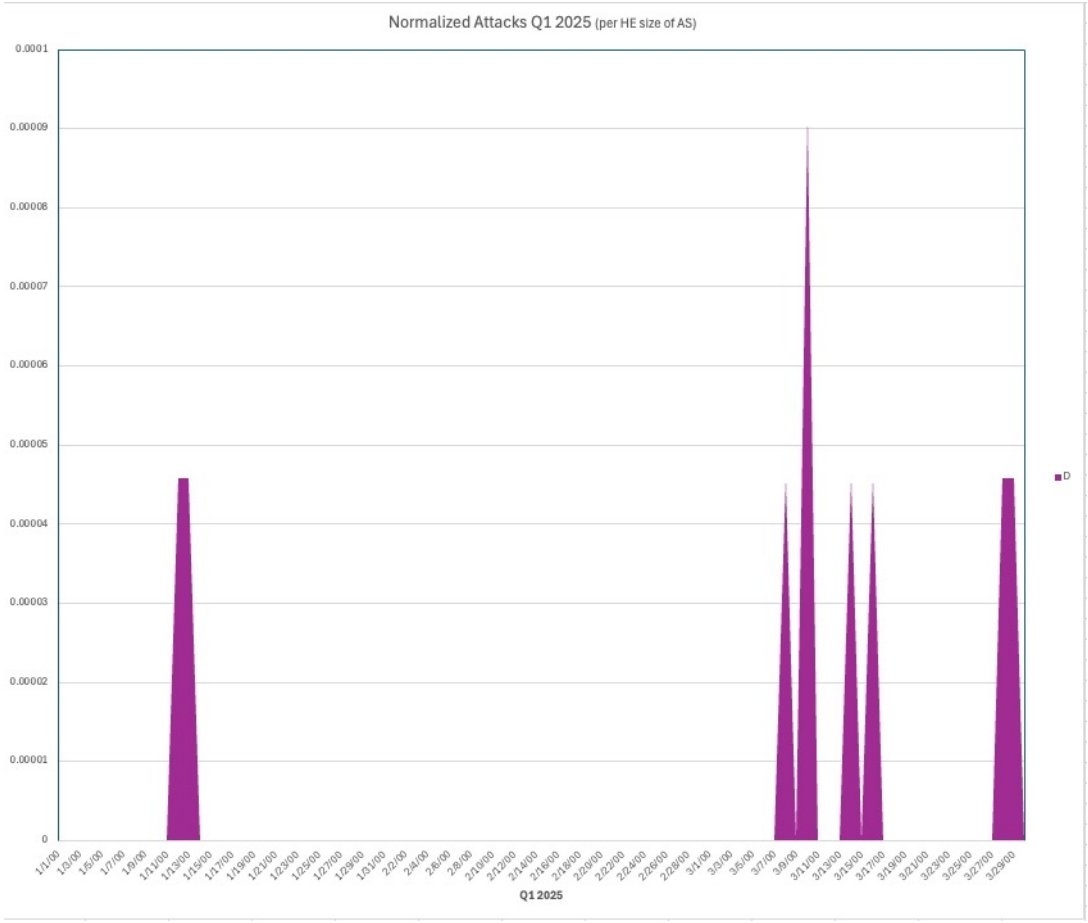
- Since 2018, GCA has been collecting data about attacks on open ports, across the globe
  - The numbers presented here are from our collected data
- In late 2024, we deployed our own honeypot sensors
  - telnet/ssh
  - http/https
  - (s)ftp
- But this talk isn't about us – it's about you, your networks, your IP addresses, and how we can (together) make them better

Global Cyber Alliance – AIDE



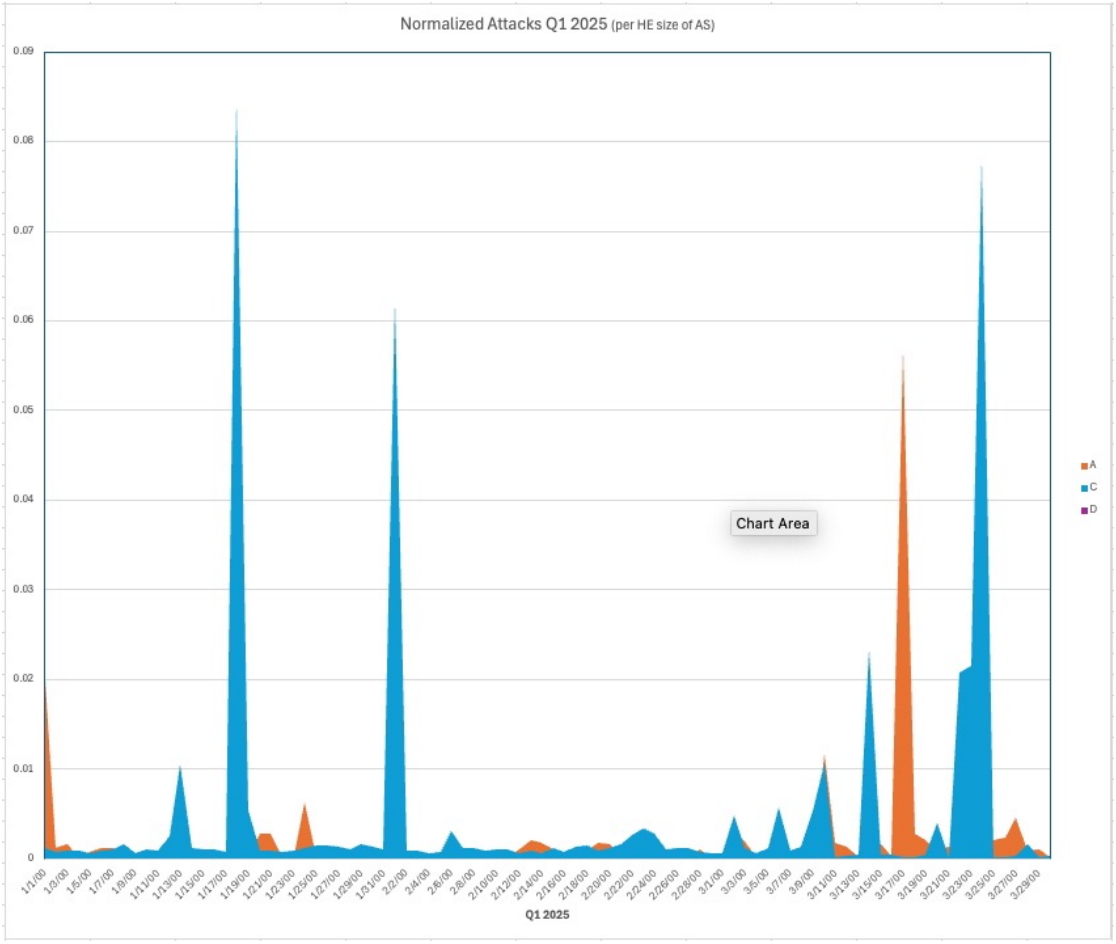
Attacks and cybersecurity challenges that arise in one part of the network **are rarely confined**, and readily impact even distant reaches of the Internet

What one network's contributions looks like from our honey farm



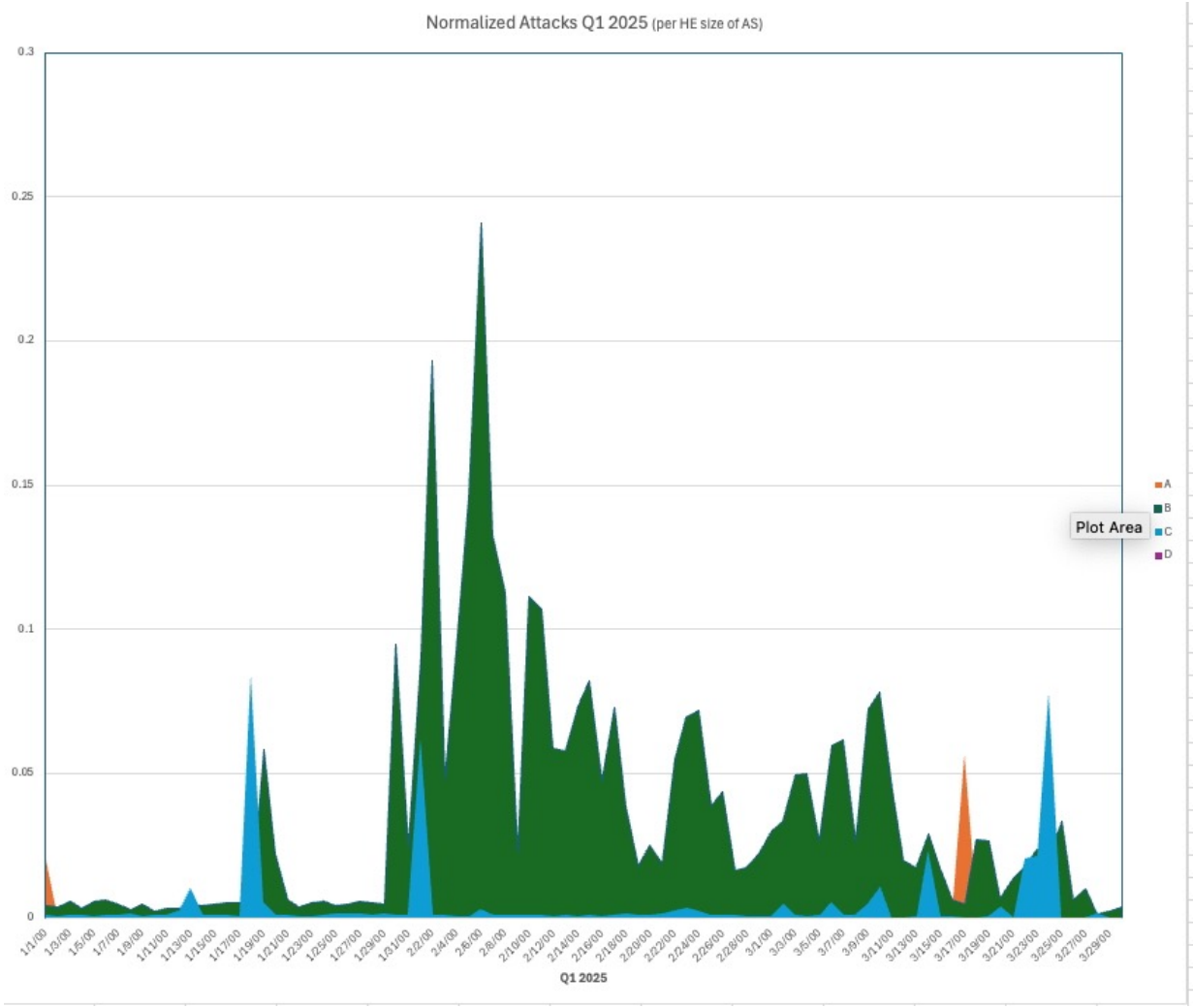
FROM ORGANIZATIONS IN THIS ROOM – Q1 2025 DAILY

A couple others were more active

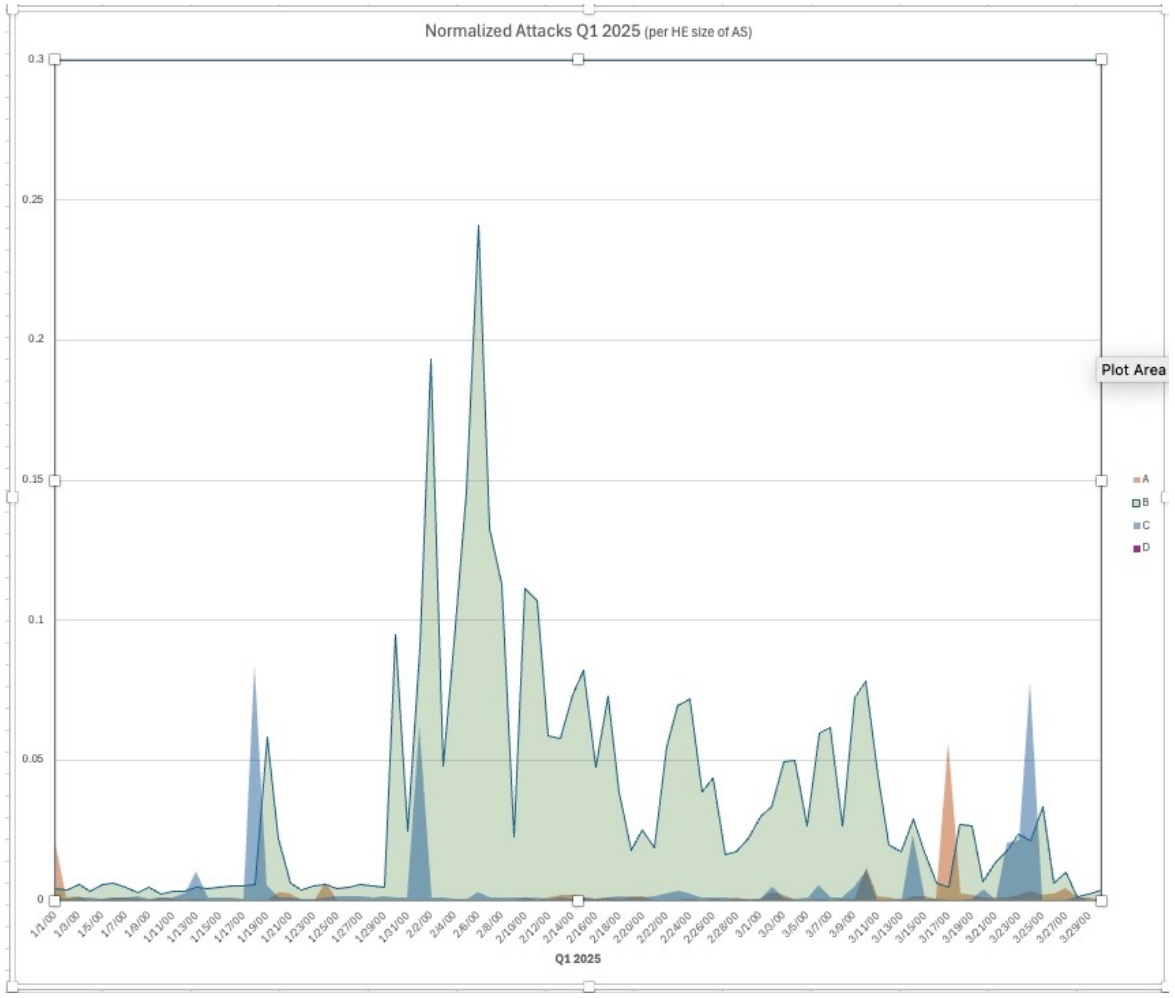


FROM ORGANIZATIONS IN THIS ROOM – Q1 2025 DAILY

Network B is clearly still working things out…

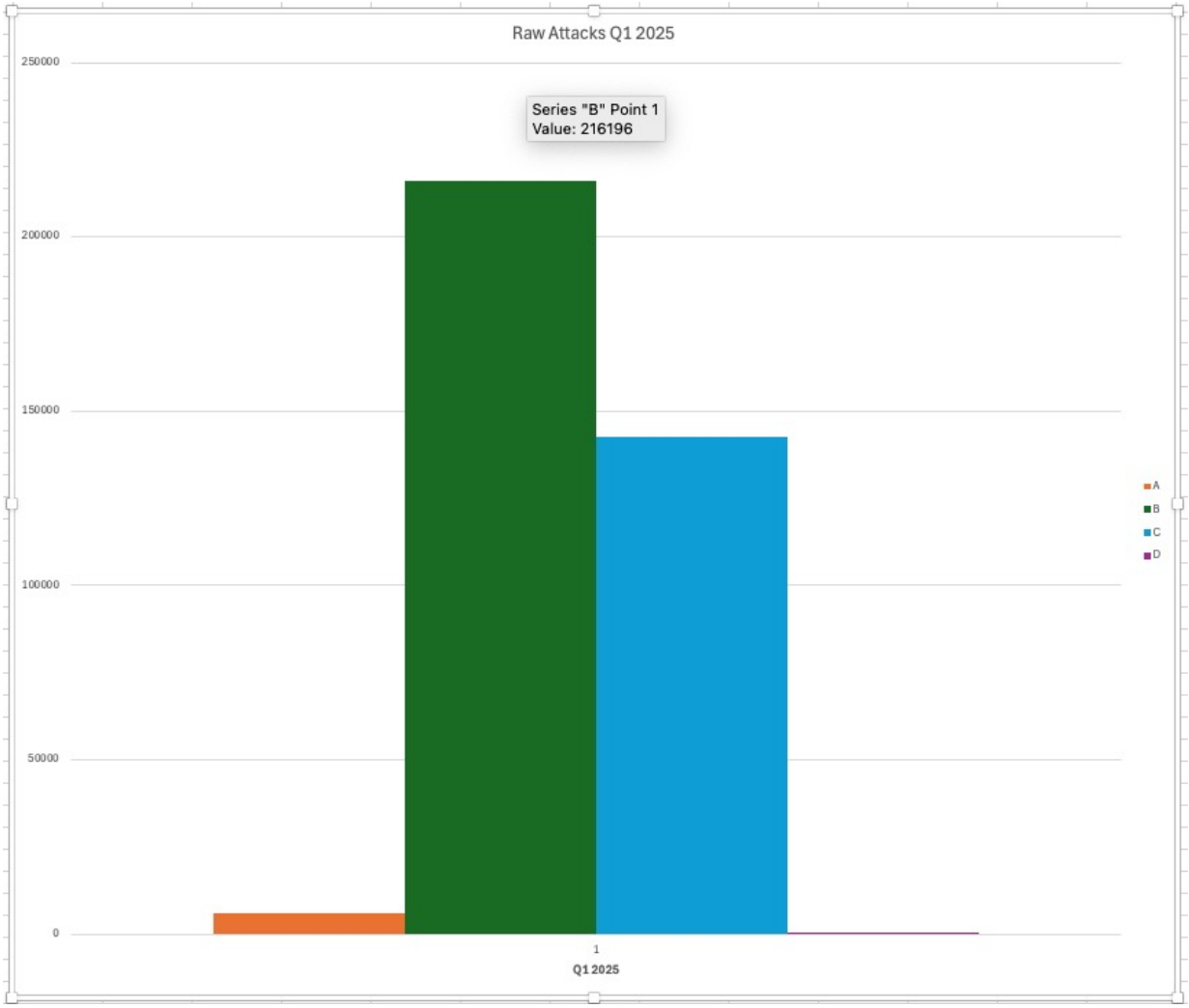


FROM ORGANIZATIONS IN THIS ROOM – Q1 2025 DAILY



FROM ORGANIZATIONS IN THIS ROOM – Q1 2025 DAILY

In sum…

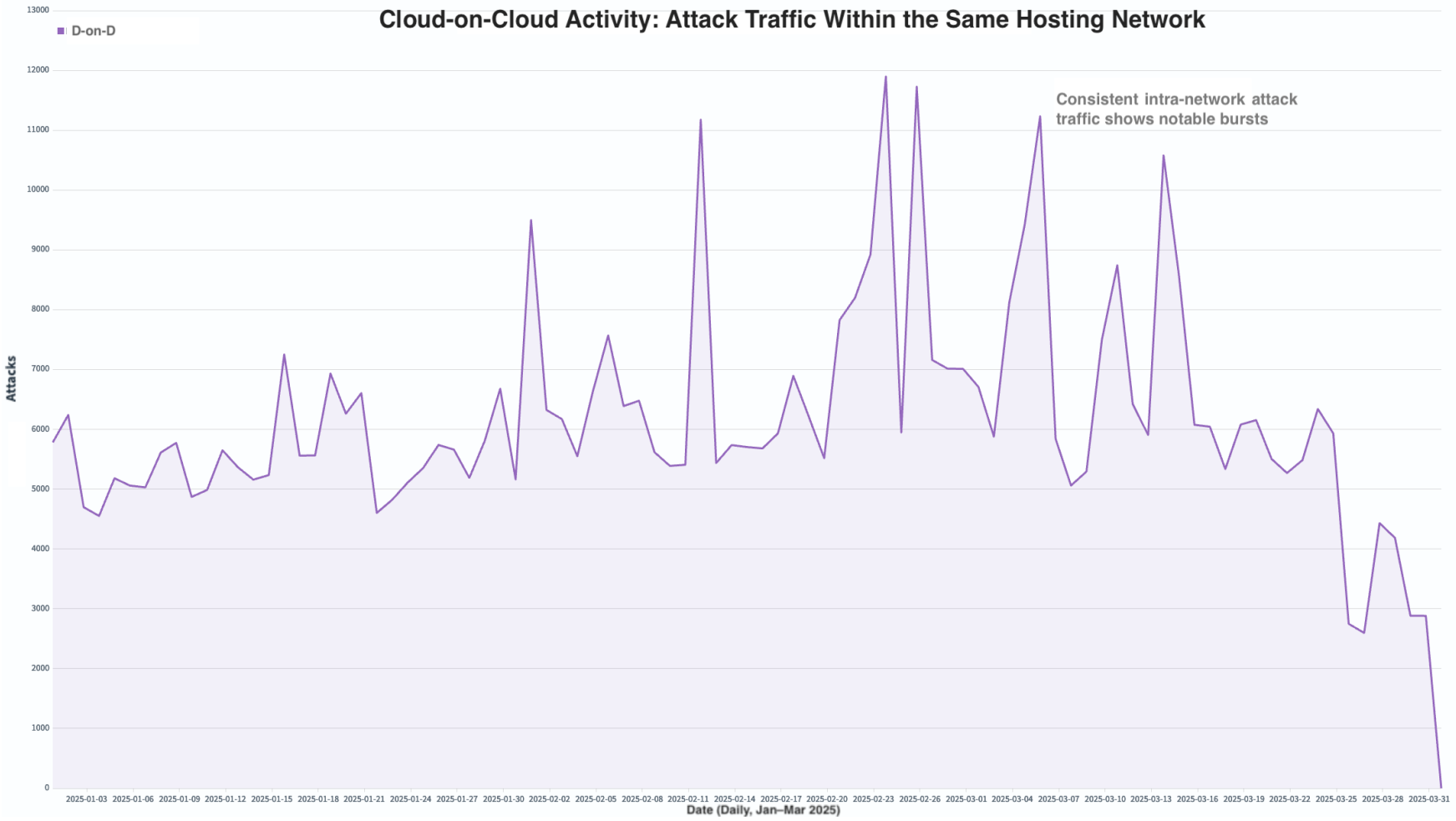


FROM ORGANIZATIONS IN THIS ROOM – Q1 2025 TOTALS

- ”It’s not impacting our bandwidth”
- ”It’s not impacting my customers”
  - Except when it is

It *is* impacting the reputation of your IP addresses.

UNWANTED TRAFFIC
THE SOURCE OF COSTLY ATTACKS

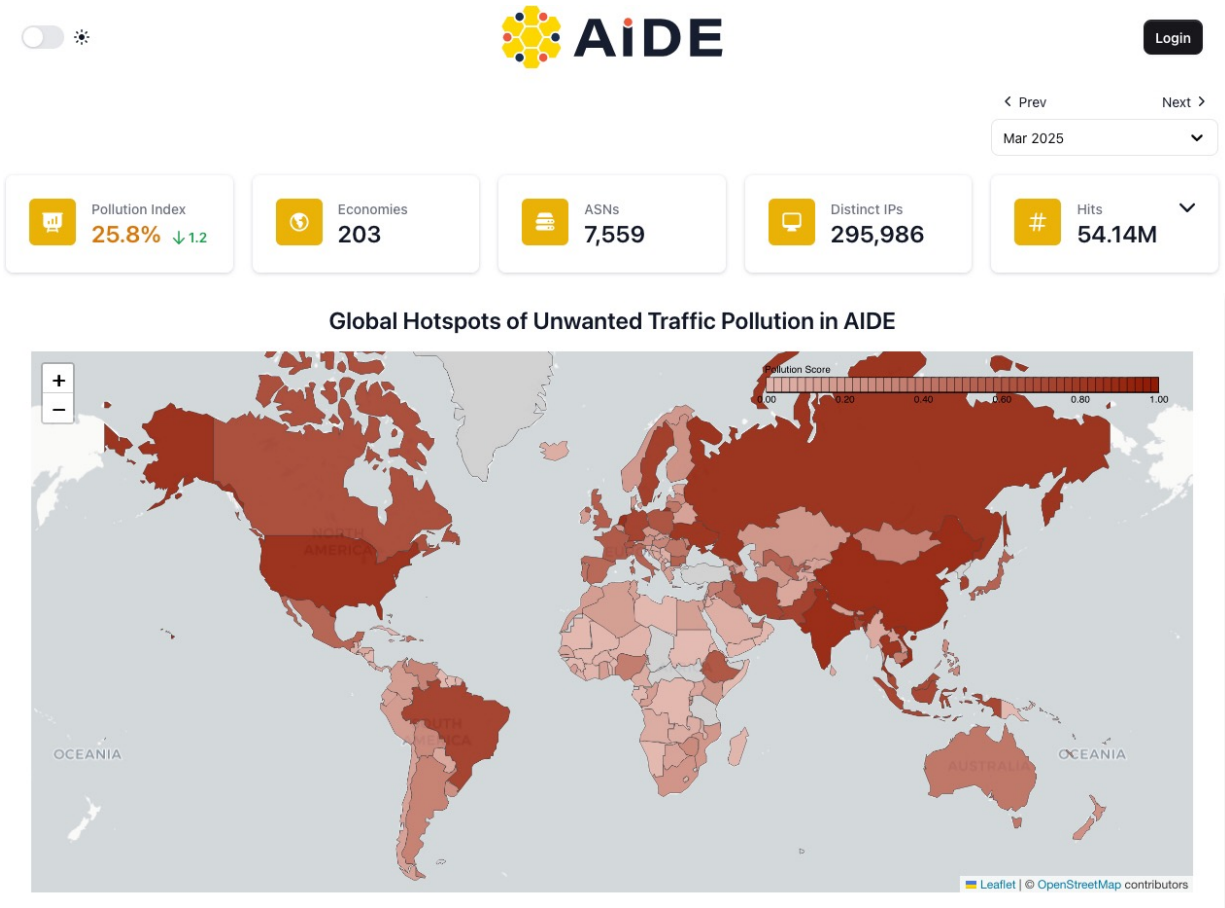


IT'S NOT IMPACTING YOUR CUSTOMERS... UNLESS IT IS

- It’s like microplastics – everywhere, and in everything
- We’re calling it “Internet Pollution”

We’ve made an Index…

UNWANTED TRAFFIC
Internet Pollution



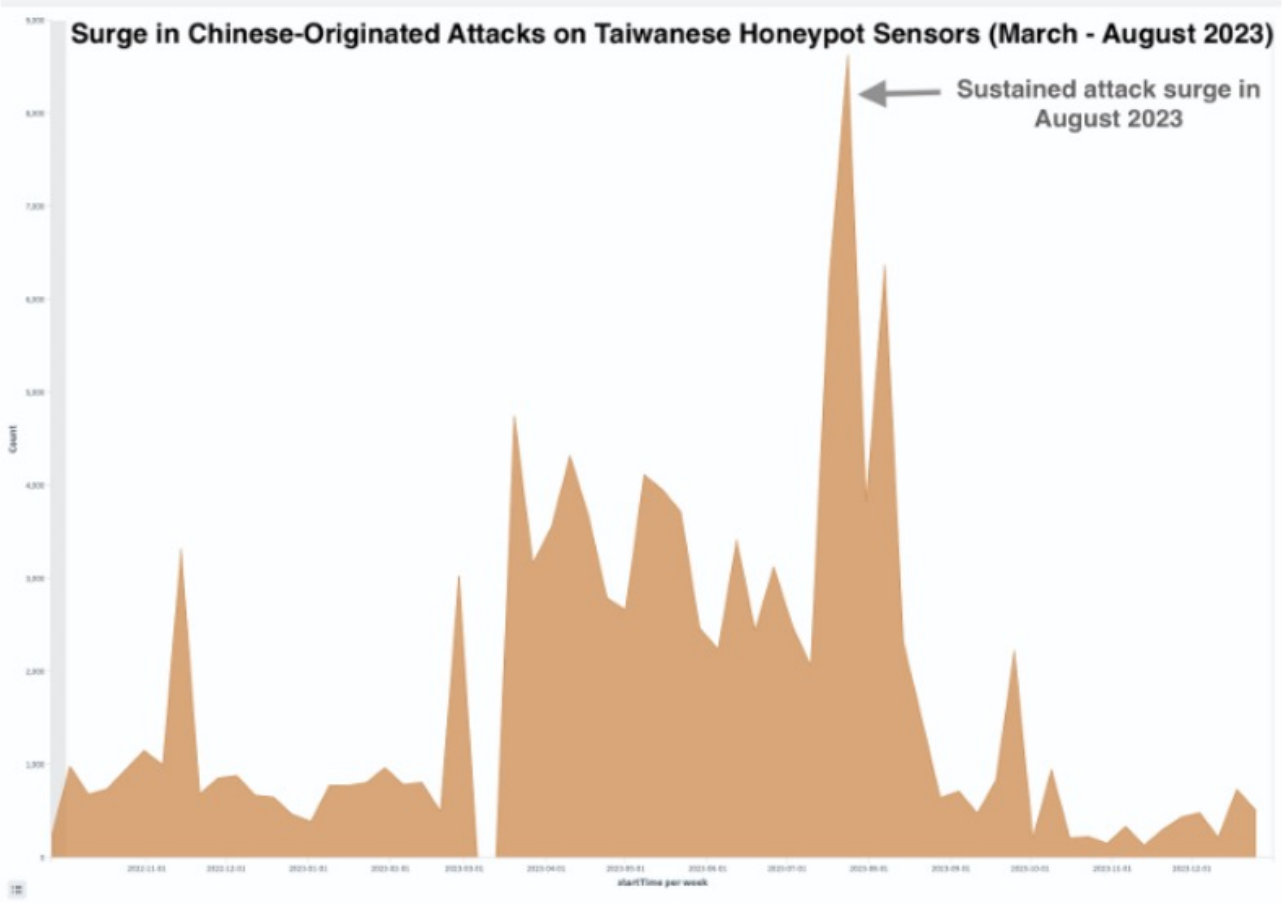
Internet Pollution Index – https://gcaaide.org


SPECIFIC ATTACK
CAMPAIGNS

- *Flax Typhoon relies on tools built into the operating system and legitimate software to remain undetected. They exploit vulnerabilities in public-facing servers, use living-off-the-land techniques, and deploy a VPN connection to maintain persistence and move laterally within compromised networks.*
- Primarily targeting Taiwan-based hardware (but the concept applies globally)

BIG IMPACT – FLAX TYPHOON

THEY'RE NOT JUST BEING FRIENDLY AND SAYING "HELLO"



FLAX TYPHOON

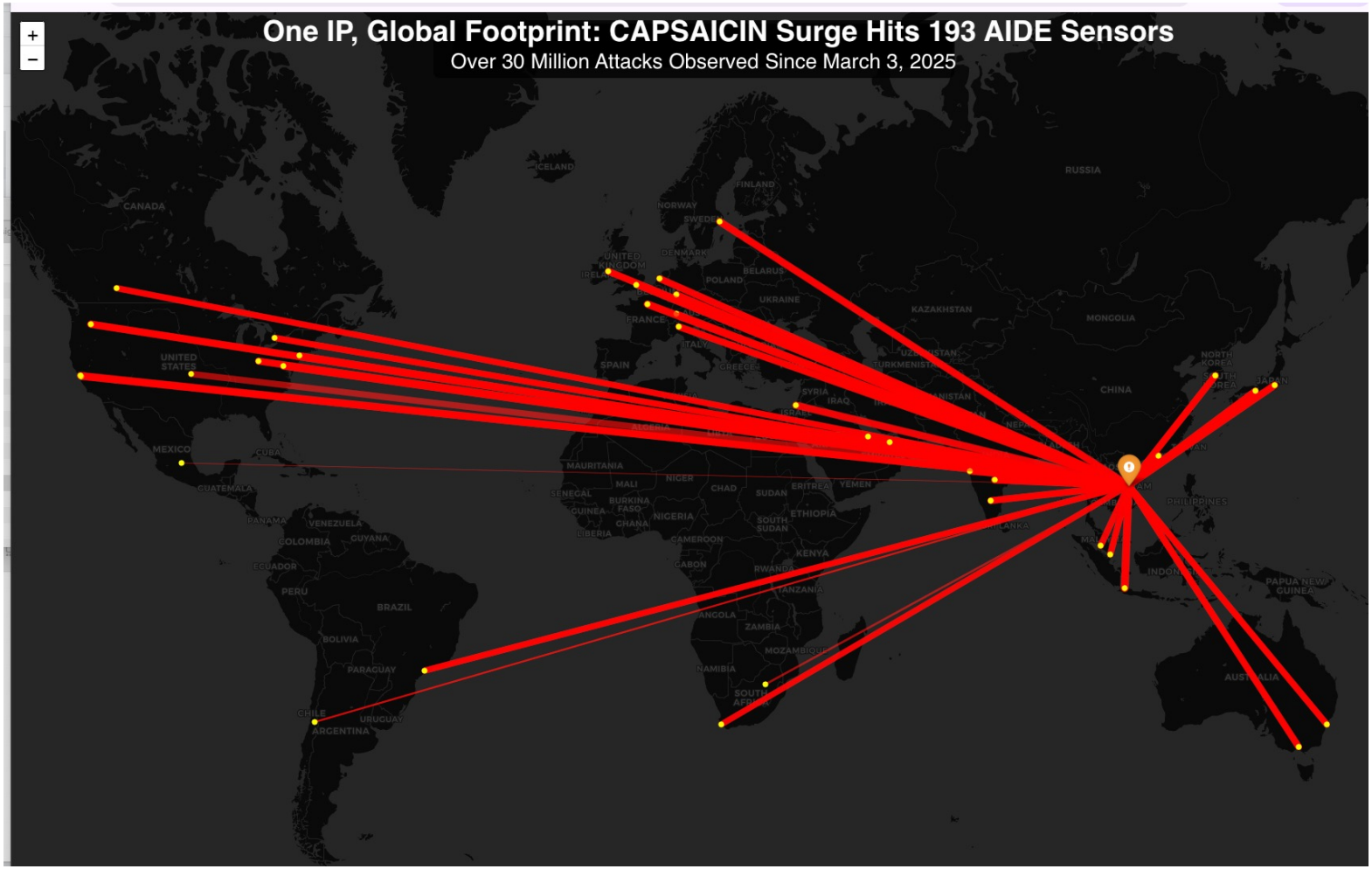
- *Cybersecurity researchers are warning about a spike in malicious activity that involves roping vulnerable D-Link routers into two different botnets, a Mirai variant dubbed FICORA and a Kaiten (aka Tsunami) variant called CAPSAICIN.*

- (Still) exploiting old D-Link vulnerabilities – those devices are still out there and getting p0wned.

- We examined an unusual spike in Telnet traffic in our data
  - the activity strongly resembled patterns used by botnets targeting vulnerable devices
  - in particular, the tactics aligned with CAPSAICIN, a variant of the Kaiten (Tsunami) botnet, and FICORA, a Mirai-based offshoot. We refer to this event as the CAPSAICIN-linked surge, based on behavioral similarities and the scale of what we observed.

BIG IMPACT – CAPSAICIN

THEY'RE NOT JUST BEING FRIENDLY AND SAYING "HELLO"

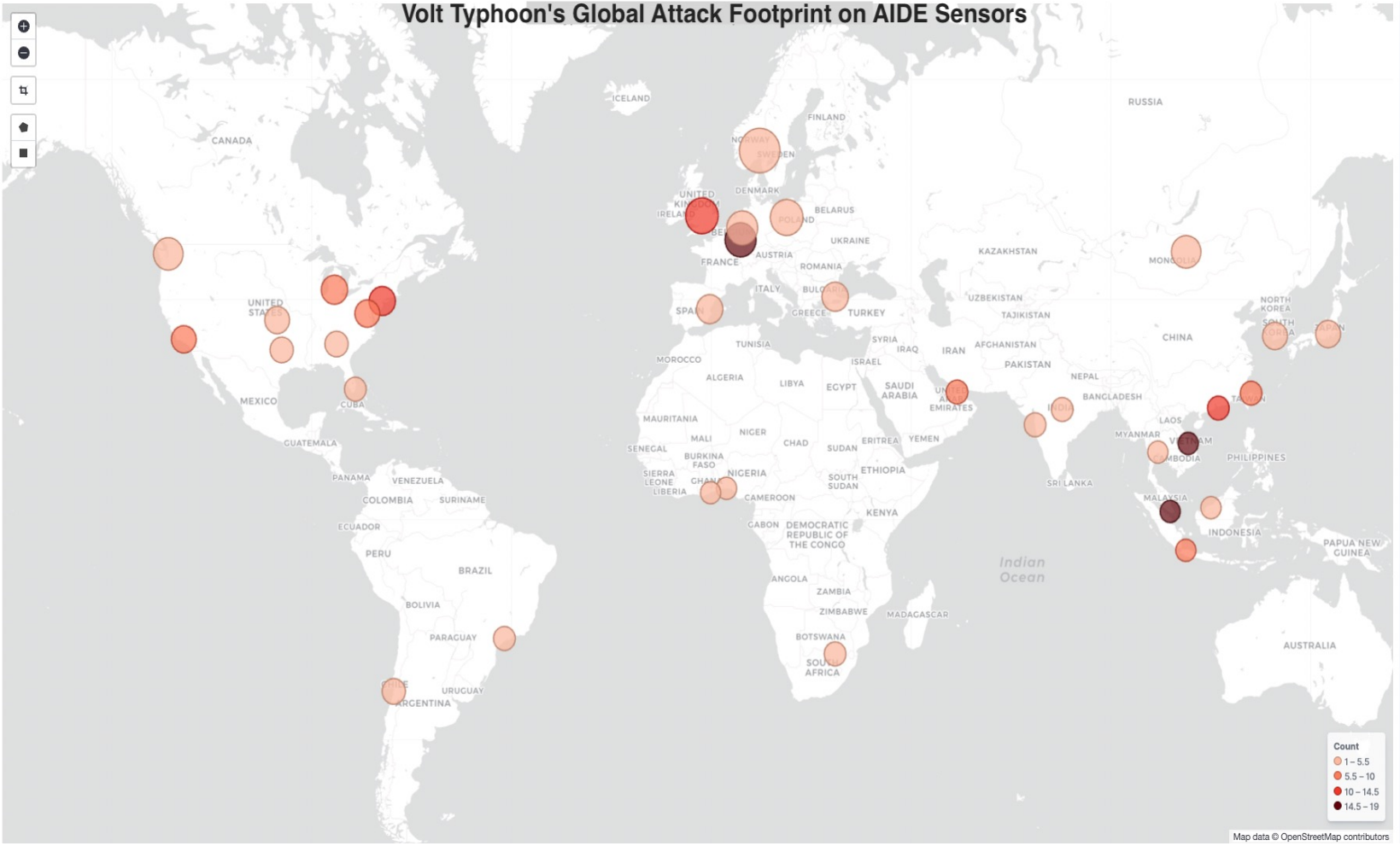


CAPSAICIN – from a single IP address

- April 2024
  - *'China is developing the "ability to physically wreak havoc" on U.S. critical infrastructure and its hackers are waiting "for just the right moment to deal a devastating blow", FBI Director Christopher Wray said on Thursday.'*
  - Campaign to take control of vulnerable routers, modems, cameras around the globe

BIG IMPACT – VOLT TYPHOON

THEY'RE NOT JUST BEING FRIENDLY AND SAYING "HELLO"



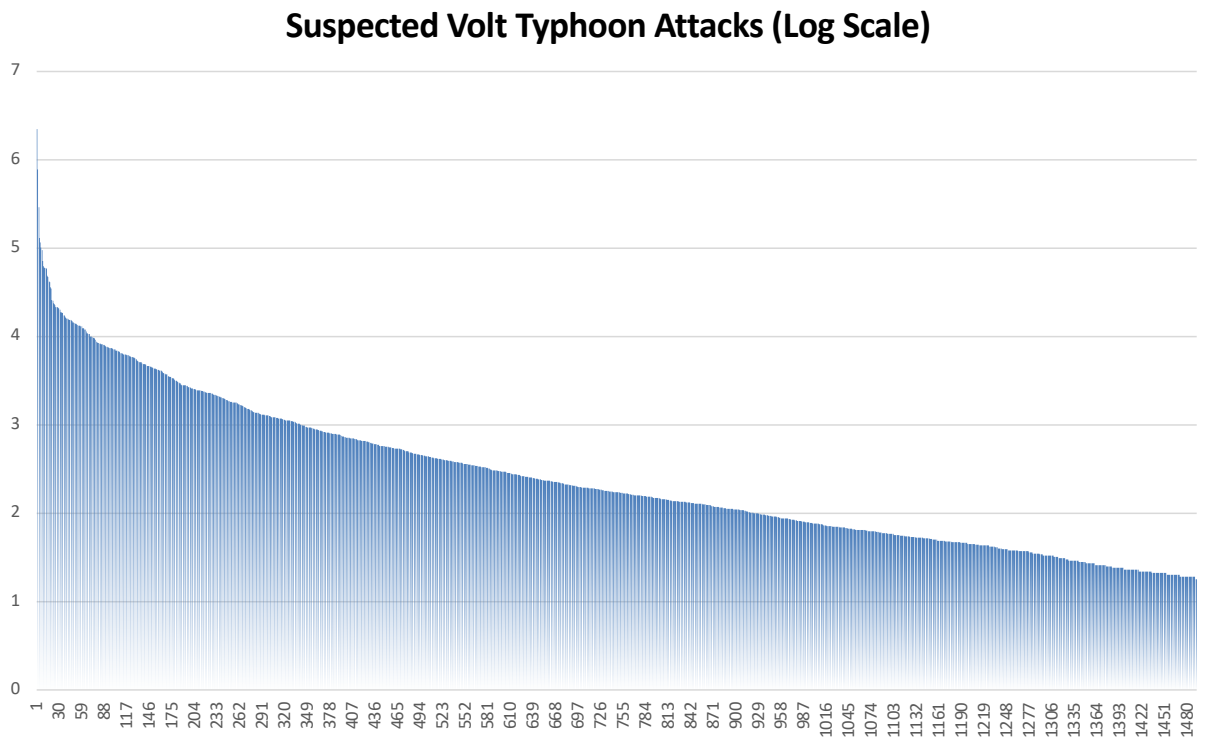
VOLT TYPHOON


VOLT TYPHOON – our
additional perspective

Log scale – max number of hits was 2,234,436 from one AS

Only showing where we saw more than 10 attacks from the AS

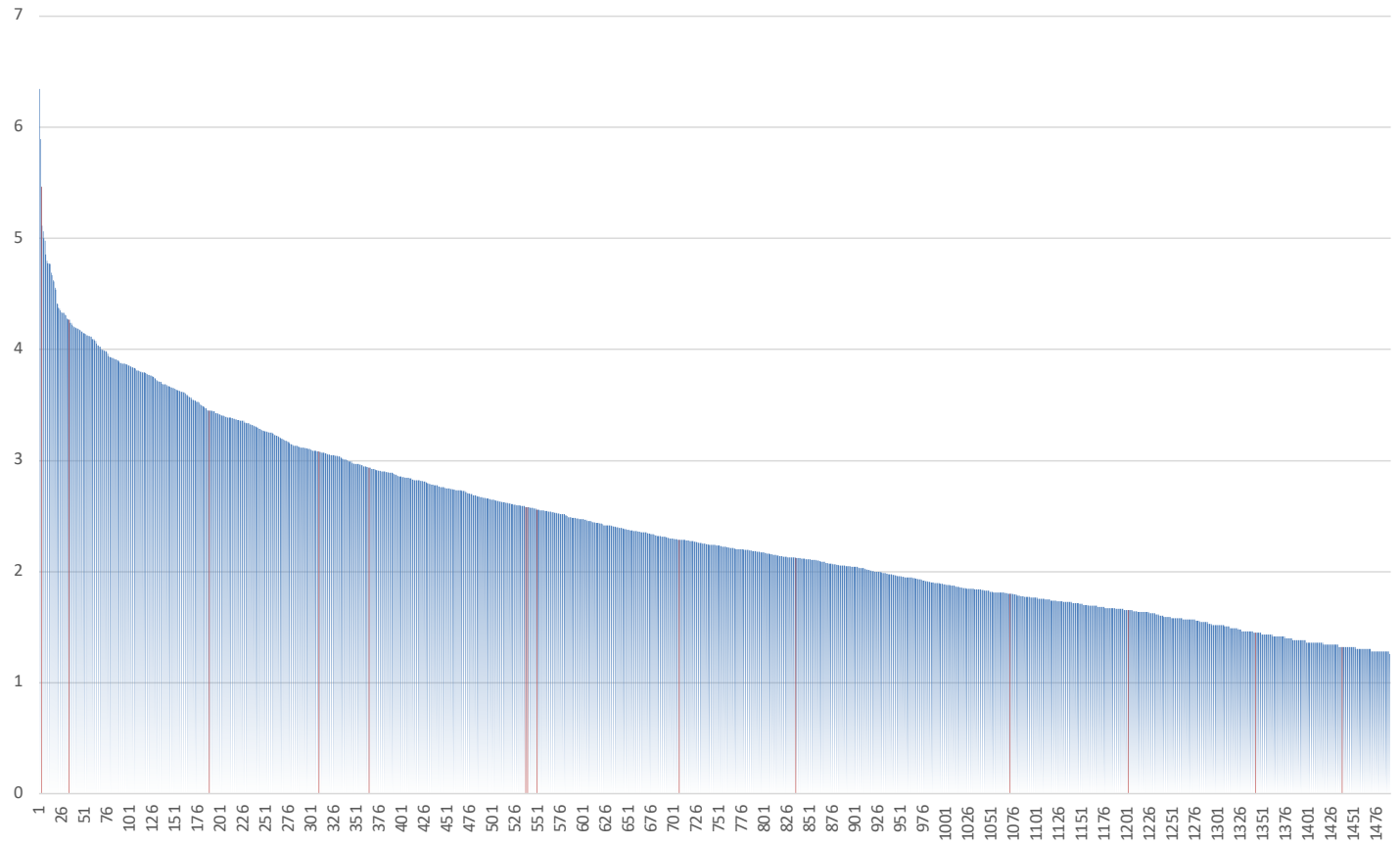
There were over 3,400 ASes in our “suspected attack” data



VOLT TYPHOON – suspected additional attacks in our data

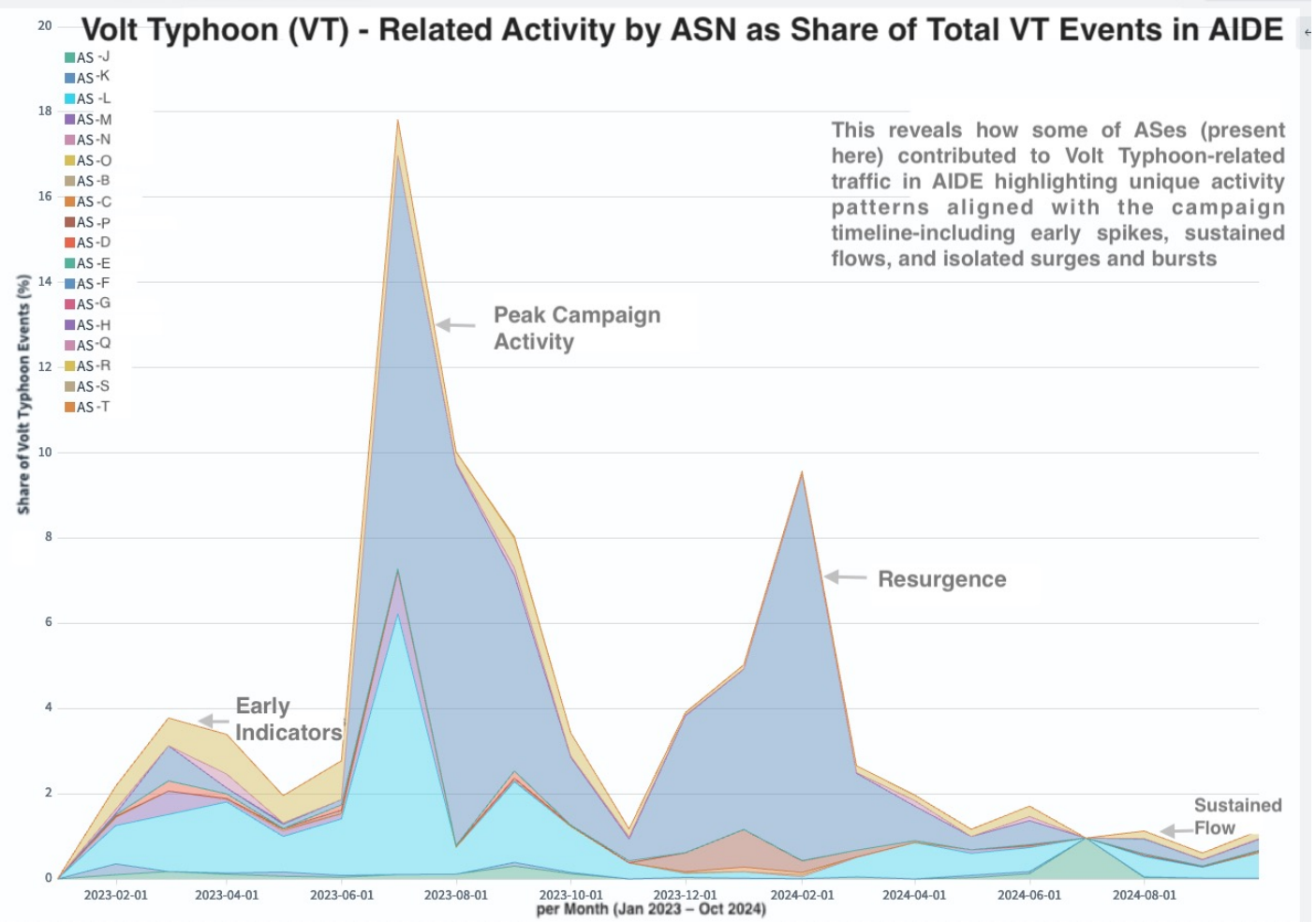
Some of your networks are showing in this list

Many of your networks are not.

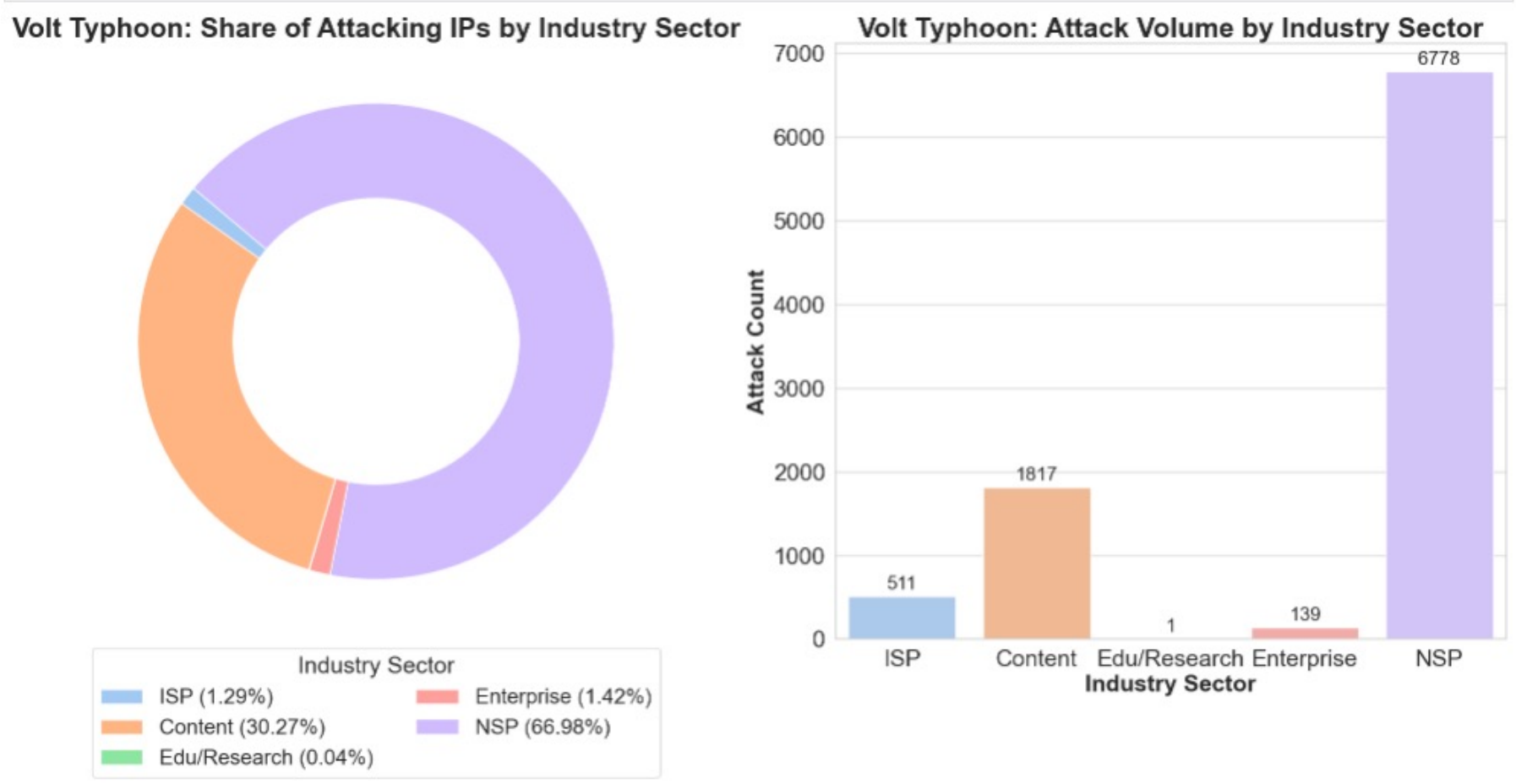


VOLT TYPHOON – suspected additional attacks in our data

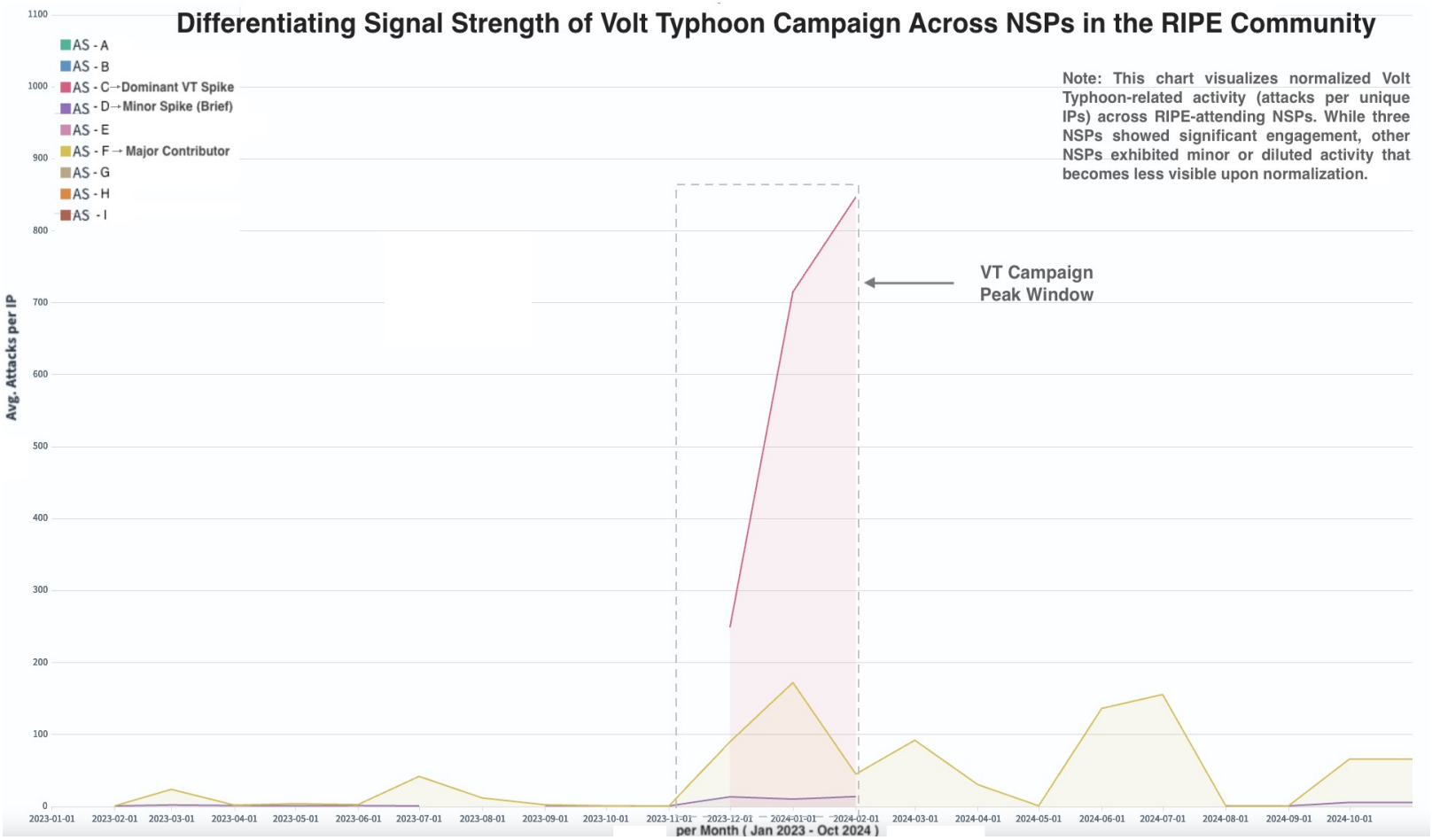
These networks are attending this meeting



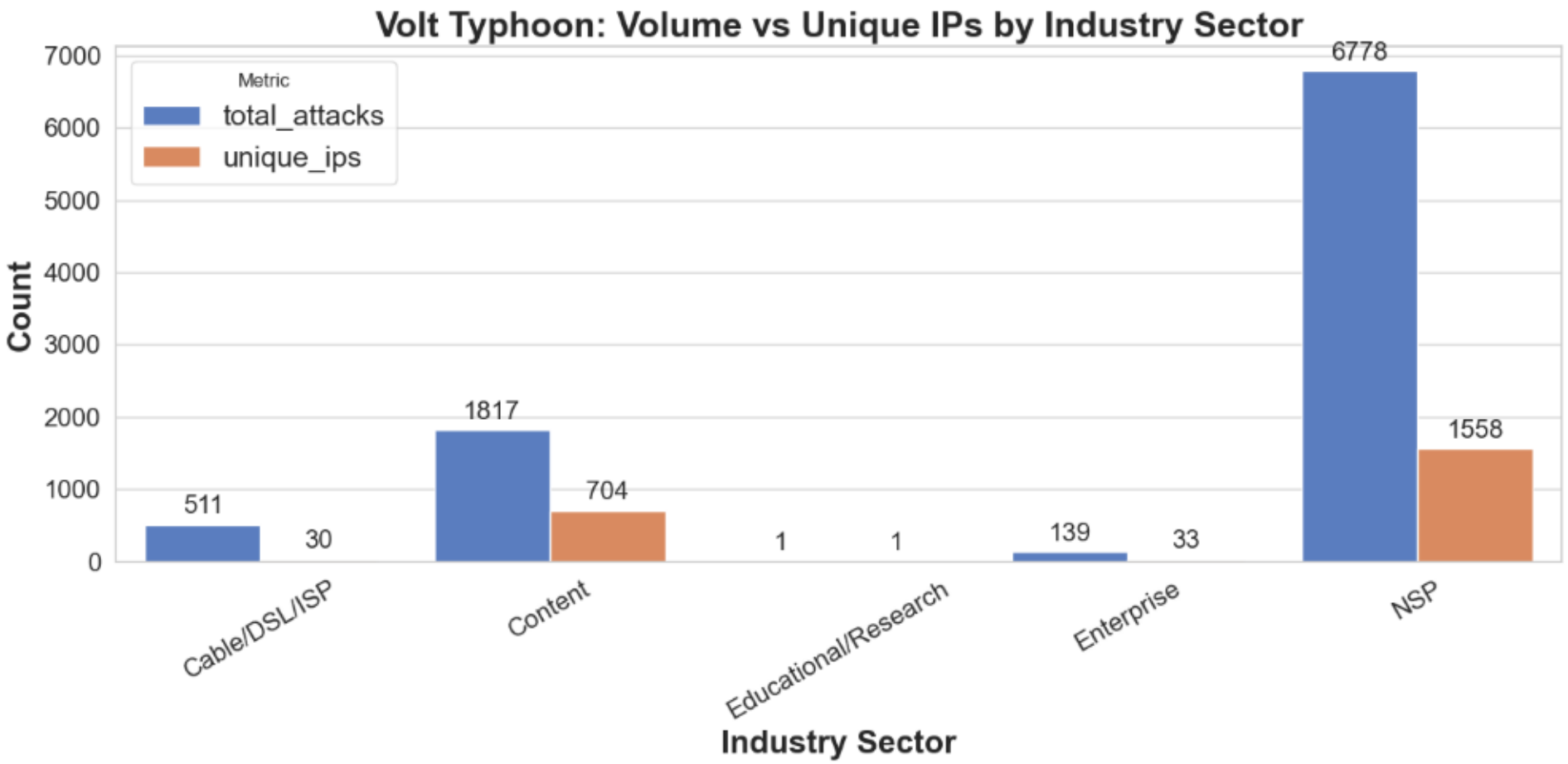
VOLT TYPHOON – suspected additional attacks in our data



VOLT TYPHOON – suspected additional attacks in our data

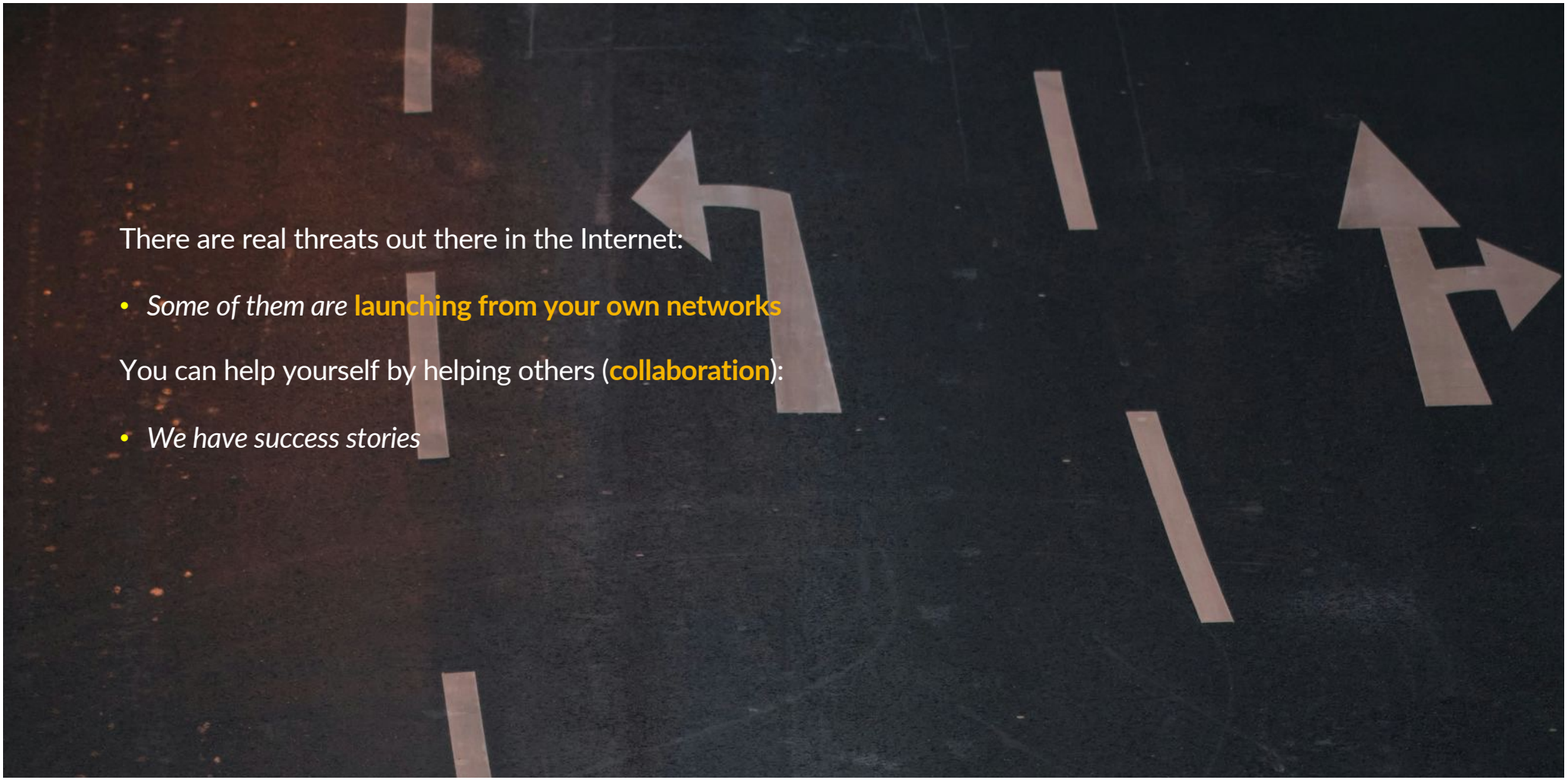


VOLT TYPHOON – suspected additional attacks in our data

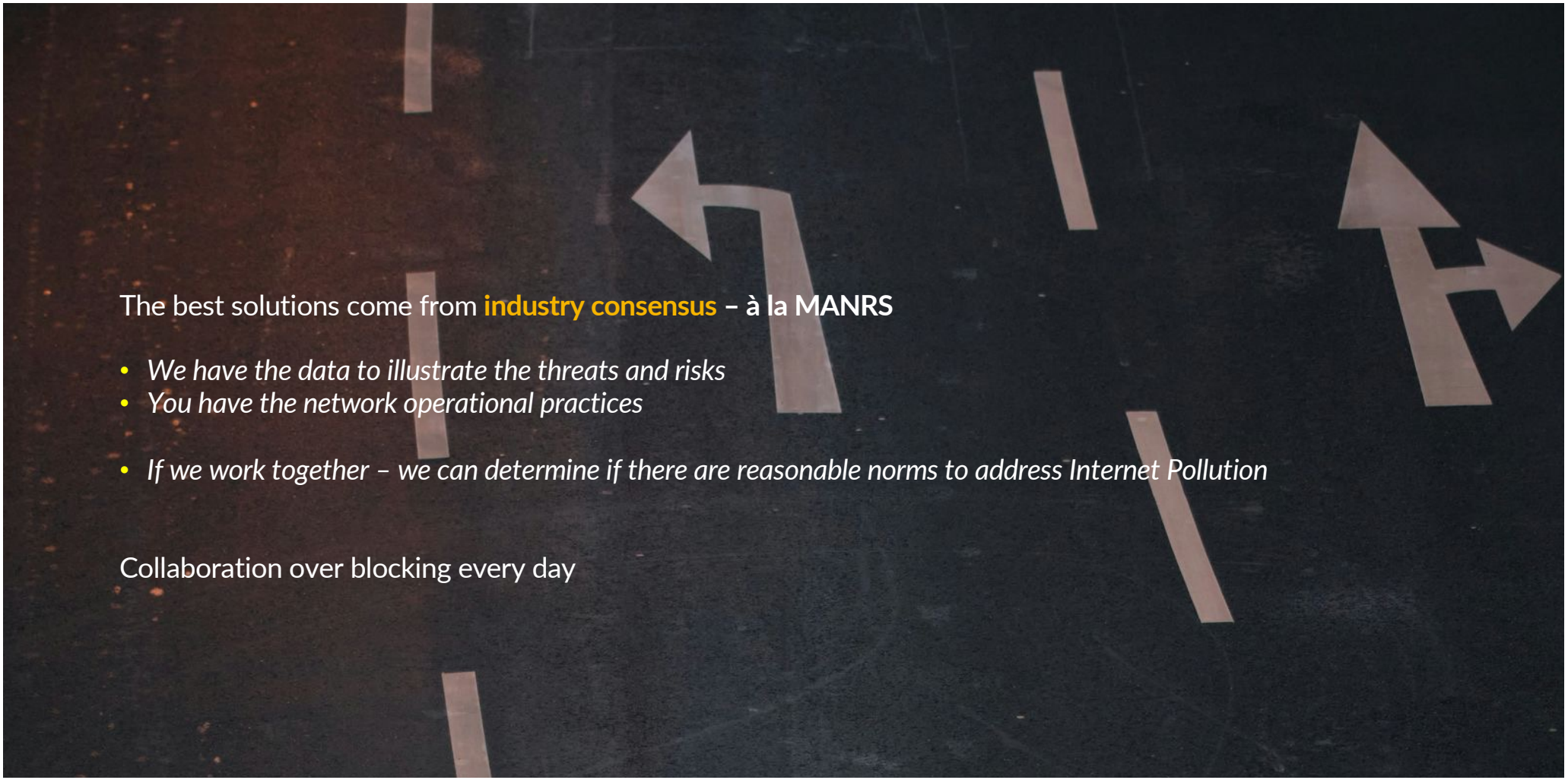


VOLT TYPHOON – suspected additional attacks in our data


Conclusions and
Takeaways



CONCLUSIONS AND TAKEAWAYS



CONCLUSIONS AND TAKEAWAYS

THANK YOU!

ldaigle@globalcyberalliance.org

Some references

- Volt Typhoon
  - https://www.reuters.com/technology/what-is-volt-typhoon-alleged-china-backed-hacking-group-2023-05-25/
- Flax Typhoon
  - https://malpedia.caad.fkie.fraunhofer.de/actor/flax_typhoon
  - More GCA analysis:
    - https://globalcyberalliance.org/flax-typhoon-aide/
- Ficora and Kaiten (CAPSAICIN)
  - https://thehackernews.com/2024/12/ficora-and-kaiten-botnets-exploit-old-d.html