STRENGTHENING INTERNET SECURITY

COLLABORATIVE SOLUTIONS FOR CYBERSECURITY CHALLENGES

LESLIE DAIGLE, GLOBAL CYBER ALLIANCE

April 28, 2025, Charlotte (NC), ARIN 55

- Securing the Internet is
  - Hard
  - A collective action problem
  - Important

- Attack campaigns are playing out on the Internet
  - Small bot traffic
  - Big security impact
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

The Internet is built on collaboration and interdependence. Its power comes from harnessing small efforts by connected networks to achieve global impact— from high quality video calls across the planet to enabling e-commerce, both scale and results are achieved by coordinated shared action.

While that produces an incredibly powerful and versatile platform for supporting commerce and communications, it also means that **attacks and cybersecurity challenges that arise in one part of the network are rarely confined** and readily impact even distant reaches of the Internet.

COLLABORATION & INTERDEPENDENCE, FOR GOOD... AND BAD

INTERNET INTEGRITY

- **Securing the Internet is**
  - **Hard**
  - A collective action problem
  - Important

- Attack campaigns are playing out on the Internet
  - Small bot traffic
  - Big security impact
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

- The Internet defined this concept, before there was an award-winning 2022 movie ;)

- In order to be able to sit in Charlotte and have a video chat back home with no noticeable lag... we built a network that:

  - *Is physically oblivious to jurisdictional boundaries*
  - *Has (domain) names that can be registered anywhere*
  - *Relies on hosting resources that may be established anywhere and replicated everywhere*

- **You can't secure this by trying to put it in a box. Any box.**

INTERNET INTEGRITY

EVERYTHING, EVERYWHERE, ALL AT ONCE

While you can impose cybersecurity mandates within your own networks, sometimes the problems come from outside your organization.

Just like maintaining highways, and preventing flooding impacts, **collective efforts and thoughtful planning by experts is imperative for maximizing cybersecurity of the Internet**.

[*Did I mention it's hard? ; -)*]

YOU ARE DEPENDENT ON THE PROPER PRACTICES OF OTHERS

- Normally, we secure things by putting boundaries around them:

  - *Locks on doors*
  - *Firewalls on networks*

- For the Internet as a whole, we need integrity and confidence in the underlying layers in order to ensure that everything riding on top can be secured

  - *Plus – everything is interconnected*
  - *Minus – everything is interconnected… and it's hard*

- You can't 2FA your way out of a routing hijack

- **As a network operator, you have to think beyond your own network (for impact, and for threats)**

INTERNET INTEGRITY

9

WHAT IS 'SECURING THE INTERNET'… WITH INTEGRITY?

- **Whose job is it to stop criminal activity on the Internet?**

  - *And, I mean Internet, not web-based applications and services*
  - *Which policy makers, if policy is to be made? What policies work*

- Different services involved; different jurisdictions:

  - *Where resources are registered?*
  - *Where resources are put into use? (hosting, networking)*
  - *Where the bad actor actually is?*

- What you see at one vantage point may not seem threatening

INTERNET INTEGRITY
WHY IS IT HARD TO SECURE THE INTERNET?

- **Securing the Internet is**
  - Hard
  - **A collective action problem**
  - Important

- Attack campaigns are playing out on the Internet
  - Small bot traffic
  - Big security impact
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

- Wide-reaching problems:
  - **Bad actors can be anywhere**

- Elusive solutions:
  - **No one organization can solve the problem for itself – collective action is required**
  - *Additionally, most solutions have ripple-effect cost and effort implications (negative externalities)*

- Unilateral mandates don't work:
  - *Legal: no single jurisdiction covers the implicated entities*
  - *Technical: every network is unique*

- Change has to happen at the level of network services:
  - *But it can't be uncoordinated –* **collective action**

INTERNET INTEGRITY
WHY SECURING THE INTERNET IS HARD?

- **Securing the Internet is**
  - Hard
  - A collective action problem
  - **Important**

- Attack campaigns are playing out on the Internet
  - Small bot traffic
  - Big security impact
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

Well. It's something we all sort of know.

INTERNET INTEGRITY
CONCRETELY: WHY IT MATTERS?

Well. It's something we all sort of know.
But let's ask ChatGPT. Because... why not?

Well. It's something we all sort of know.
But let's ask ChatGPT. Because... why not?

Why does it matter to secure the infrastructures of the internet?

INTERNET INTEGRITY
CONCRETELY: WHY IT MATTERS?

Well. It's something we all sort of know.
But let's ask ChatGPT. Because... why not?

Why does it matter to secure the infrastructures of the internet?

A bit of prompting later...

INTERNET INTEGRITY
CONCRETELY: WHY IT MATTERS?

How Small Issues in Network Operations Lead to Large Cyberattacks

- **Misconfigured Firewalls & Access Controls → Unauthorized Access**
  - Open ports (e.g., SSH, RDP) allow brute-force attacks.
  - Attackers use tools like Shodan and Nmap to find exposed systems.
  - *Impact*: Unauthorized access, lateral movement, data breaches.
- **BGP Hijacking → Traffic Interception & Disruption**
  - Manipulating Border Gateway Protocol (BGP) can reroute internet traffic.
  - *Example*: Google's traffic was hijacked in 2018, affecting global connectivity.
  - *Impact*: Data interception, downtime, economic damage.
- **DNS Attacks → Traffic Redirection & Credential Theft**
  - DNS hijacking redirects users to fake sites for credential harvesting.
  - *Example*: 2019 attack on government agencies to steal email credentials.
  - *Impact*: Phishing, malware distribution, corporate espionage.
- **Unpatched Network Devices → Ransomware & Botnets**
  - Outdated routers, switches, and VPNs are prime targets.
  - *Example*: Mirai botnet exploited IoT devices for massive DDoS attacks.
  - *Impact*: Ransomware outbreaks, botnet recruitment, full network compromise.
- **Insecure SNMP Configurations → Network Device Takeover**
  - Publicly accessible SNMP with weak community strings exposes network data.
  - *Impact*: Unauthorized control of infrastructure, persistent threats.
- **Insufficient Segmentation → Attack Spread**
  - Lack of segmentation allows malware to spread rapidly.
  - *Example*: WannaCry ransomware propagated due to flat networks.
  - *Impact*: Large-scale data breaches, operational downtime.
- **DDoS Amplification Attacks → Service Disruptions**
  - Exploiting misconfigured services (DNS, NTP, Memcached) for massive traffic floods.
  - *Example*: 2023's largest-ever DDoS attack generated 71M requests per second.
  - *Impact*: Service outages, financial losses, reputational damage.

Well. It's someth
But let's ask Cha

Why d   nternet?

A bit of prompti

INTERNET INTEGRITY

CONCRETELY: WHY IT MATTERS?

- UnitedHealth Group said its quarterly earnings fell **BY MORE THAN A FIFTH** after a cyberattack in February on its Change Healthcare unit. The hack cost the company 92 cents a share in the second quarter, WSJ reports.
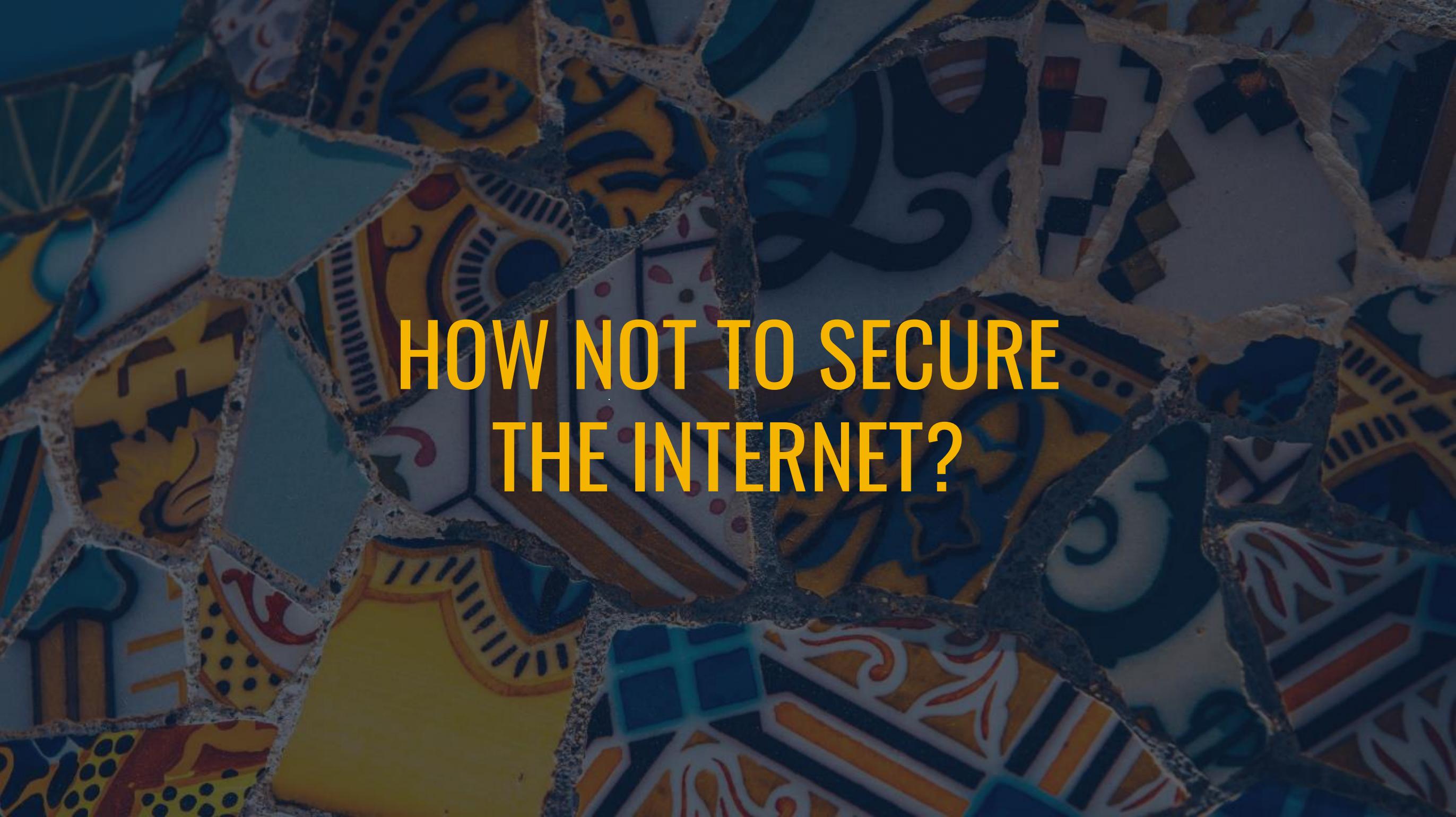
- **Every industry is impacted**, e.g., law firms.

- Cybersecurity breaches aren't just technical, **they impact business.**

- You think it's an outage, but really **it's a route hijack.**

- **Not an attack, but...** the CrowdStrike update that bricked Windows servers on July 19, 2024 illustrated clearly the extensive and pervasive reliance on global IT systems.

WHY WE (ALL) CARE ABOUT SECURING THE INTERNET?

- UnitedHealth Group said its quarterly earnings fell **BY MORE THAN A FIFTH** after a cyberattack in February on its Change Healthcare unit. The hack cost the company 92 cents a share in the second quarter, WSJ reports. 🔲www

- **Every industry is impacted**, e.g., law firms. 🔲www

- Cybersecurity breaches aren't just technical, **they impact business.** 🔲www

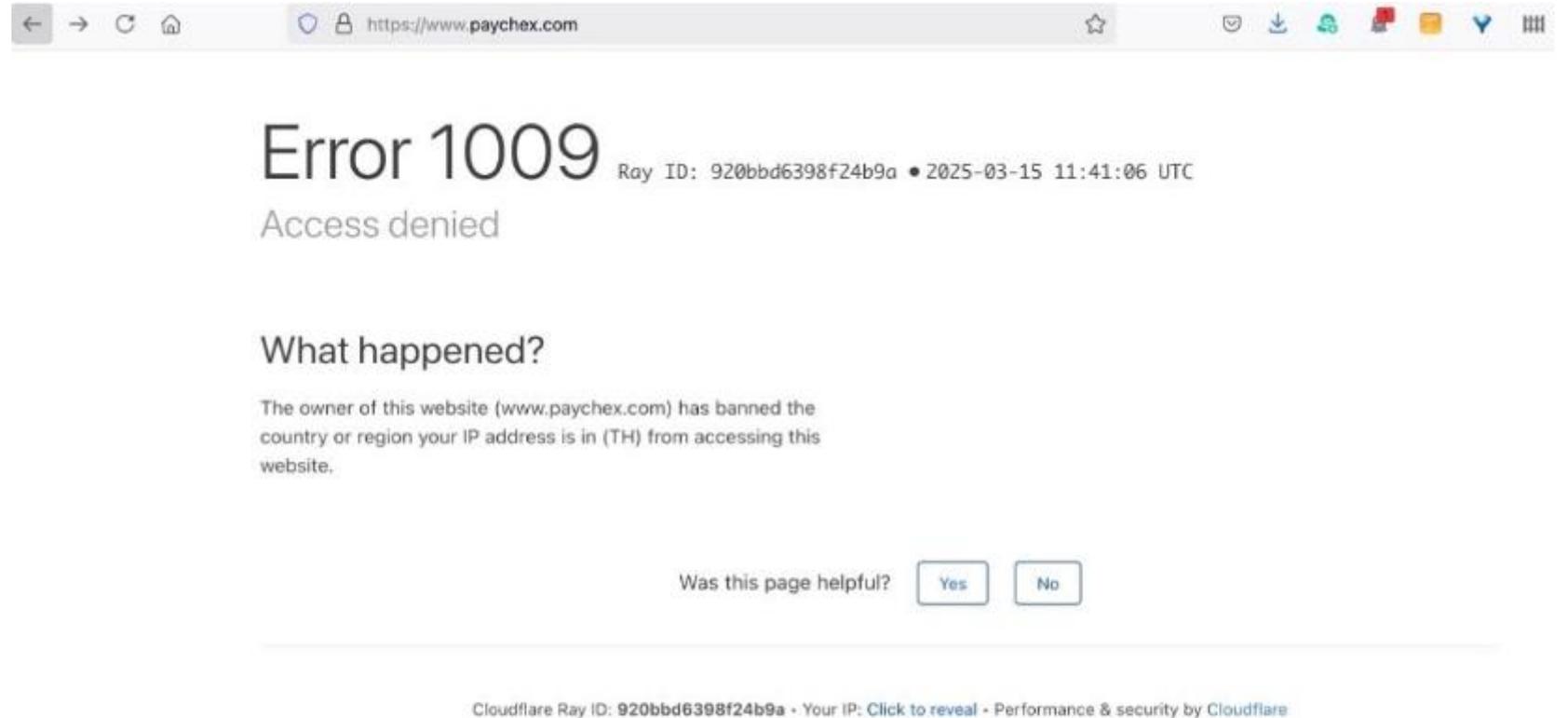- You think it's an outage, but really **it's a route hijack.** 🔲www

- **Not an attack, but...** the CrowdStrike update that bricked Windows servers on July 19, 2024 illustrated clearly the extensive and pervasive reliance on global IT systems.

WHY WE (ALL) CARE ABOUT SECURING THE INTERNET?

HOW NOT TO SECURE
THE INTERNET?

- *Too many attacks from Thailand?*

- *Regulations too hard to comply with (à la GDPR)?*

- *No use case apparent to Paychex*

- *Was this page helpful?*

← → C ⌂   🛡 🔒 https://www.paychex.com   ☆   ✉ ⬇ 👥 📌 🟨 Y ⊞

Error 1009 Ray ID: 920bbd6398f24b9a • 2025-03-15 11:41:06 UTC

Access denied

What happened?

The owner of this website (www.paychex.com) has banned the country or region your IP address is in (TH) from accessing this website.

Was this page helpful? [Yes] [No]

Cloudflare Ray ID: **920bbd6398f24b9a** • Your IP: Click to reveal • Performance & security by Cloudflare

WHAT IT LOOKS LIKE WHEN WE GET IT WRONG?

SO, THEN, WHAT?

You can't secure the Internet.

But, together we can make progress on it:

- *The Internet – as collaboration example*
- *World IPv6 Day & Launch*
- *MANRS – Mutually Agreed Norms for Routing Security*

BLUF

NAMES

data

NUMBERS   ROUTES

infrastructure

humans

INTERNET INTEGRITY
NAMES, NUMBERS, AND ROUTES

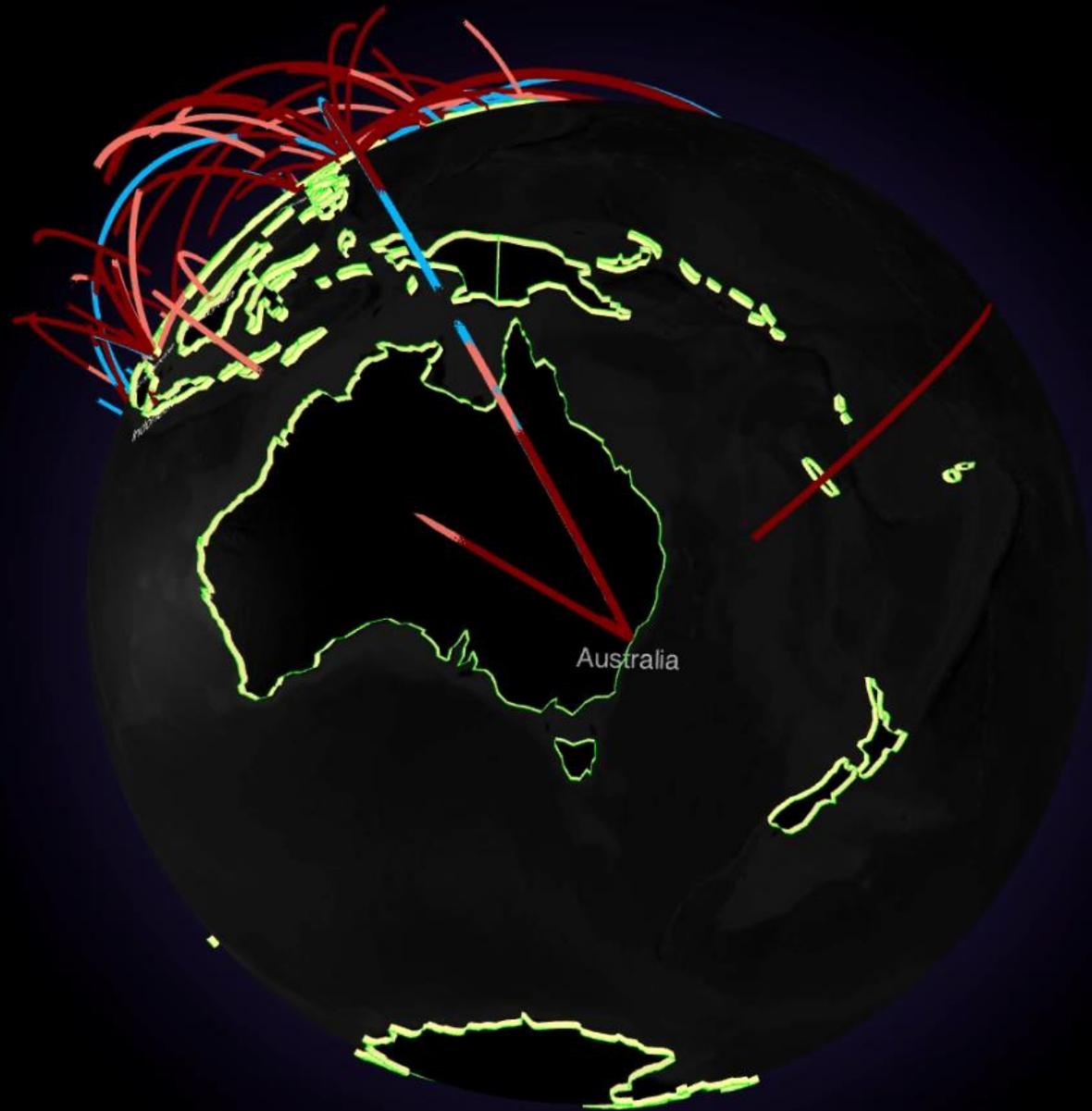INTERNET INTEGRITY
NAMES, NUMBERS, AND ROUTES

- Securing the Internet is
  - Hard
  - A collective action problem
  - Important

- **Attack campaigns are playing out on the Internet**
  - **Small bot traffic**
  - Big security impact
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

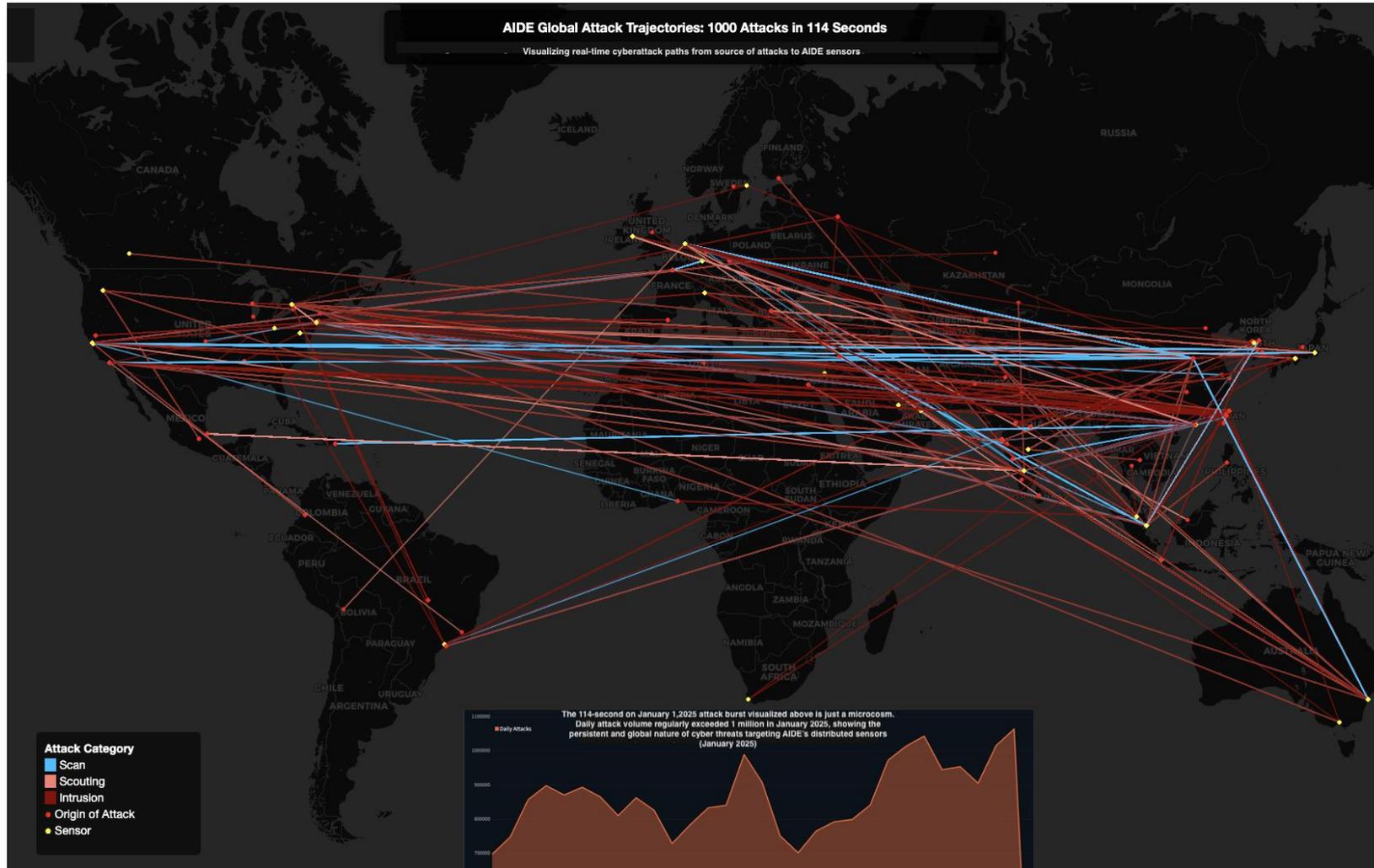- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

ATTACKS BY THE NUMBERS

Scan
Scouting
Intrusion

29

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

- Securing the Internet is
  - Hard
  - A collective action problem
  - Important

- **Attack campaigns are playing out on the Internet**
  - Small bot traffic
  - **Big security impact**
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

- 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"

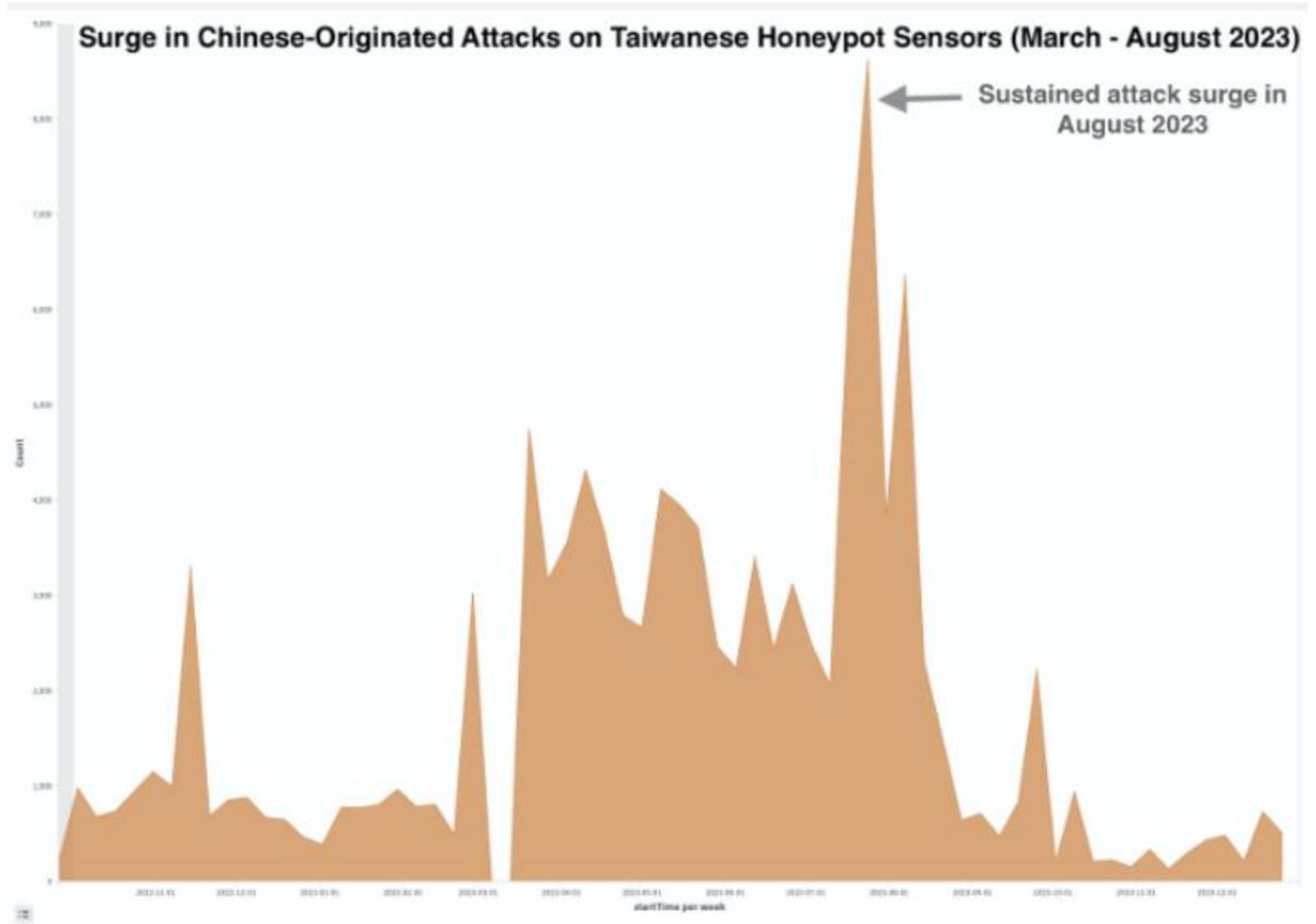Volt Typhoon's Global Attack Footprint on AIDE Sensors

VOLT TYPHOON
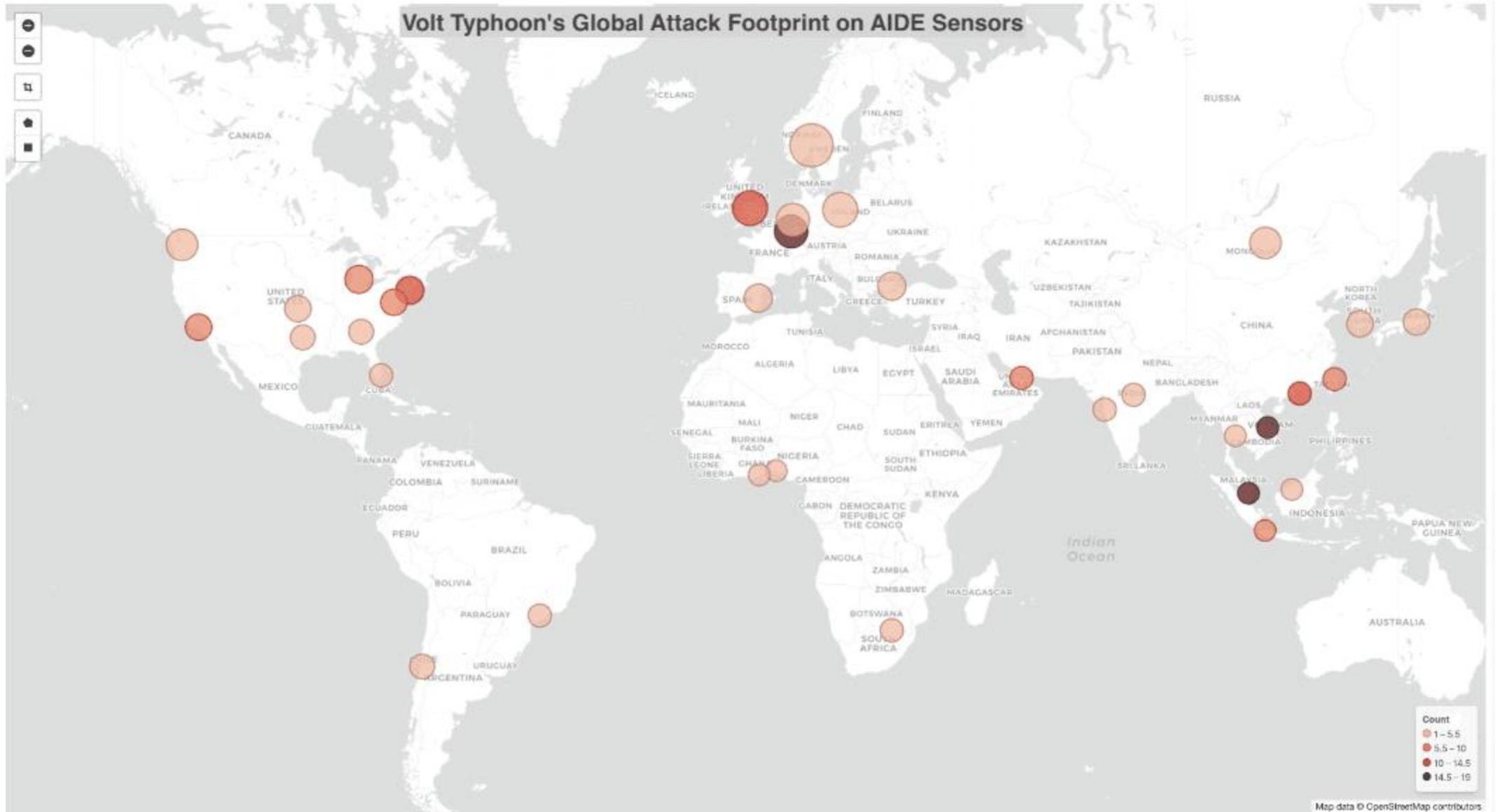
- *Flax Typhoon relies on tools built into the operating system and legitimate software to remain undetected. They exploit vulnerabilities in public-facing servers, use living-off-the-land techniques, and deploy a VPN connection to maintain persistence and move laterally within compromised networks.*

- Primarily targeting Taiwan-based hardware (but the concept applies globally)

BIG IMPACT – FLAX TYPHOON
THEY'RE NOT JUST BEING FRIENDLY AND SAYING "HELLO"

Surge in Chinese-Originated Attacks on Taiwanese Honeypot Sensors (March - August 2023)

Sustained attack surge in August 2023

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"

One IP, Global Footprint: CAPSAICIN Surge Hits 193 AIDE Sensors
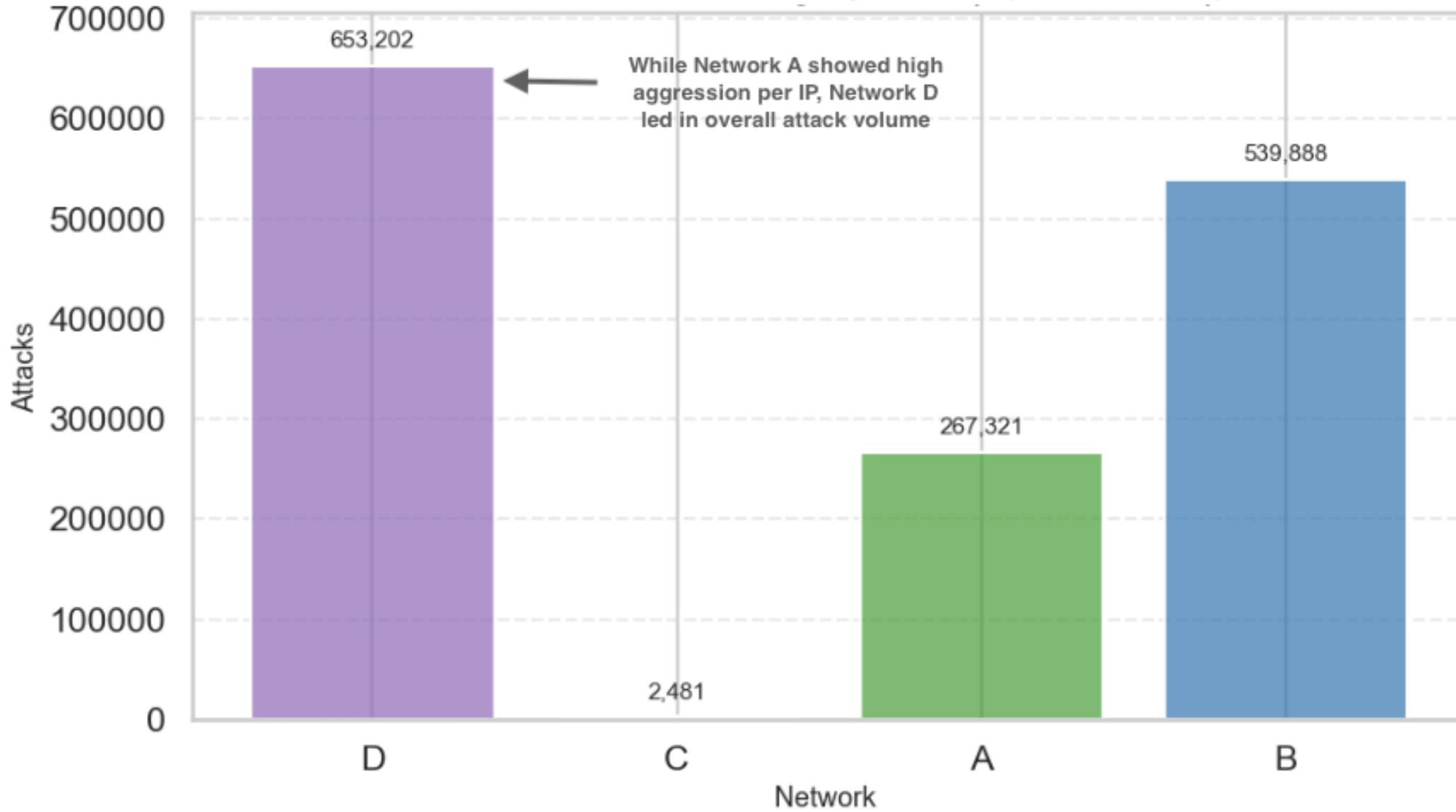Over 28 Million Attacks Observed Since March 3, 2025

CAPSAICIN – from a single IP address

- Securing the Internet is
  - Hard
  - A collective action problem
  - Important

- Attack campaigns are playing out on the Internet
  - Small bot traffic
  - Big security impact
- **We can see them**.
  - **Perhaps they can be stopped before they become multinational trans-network affairs**?

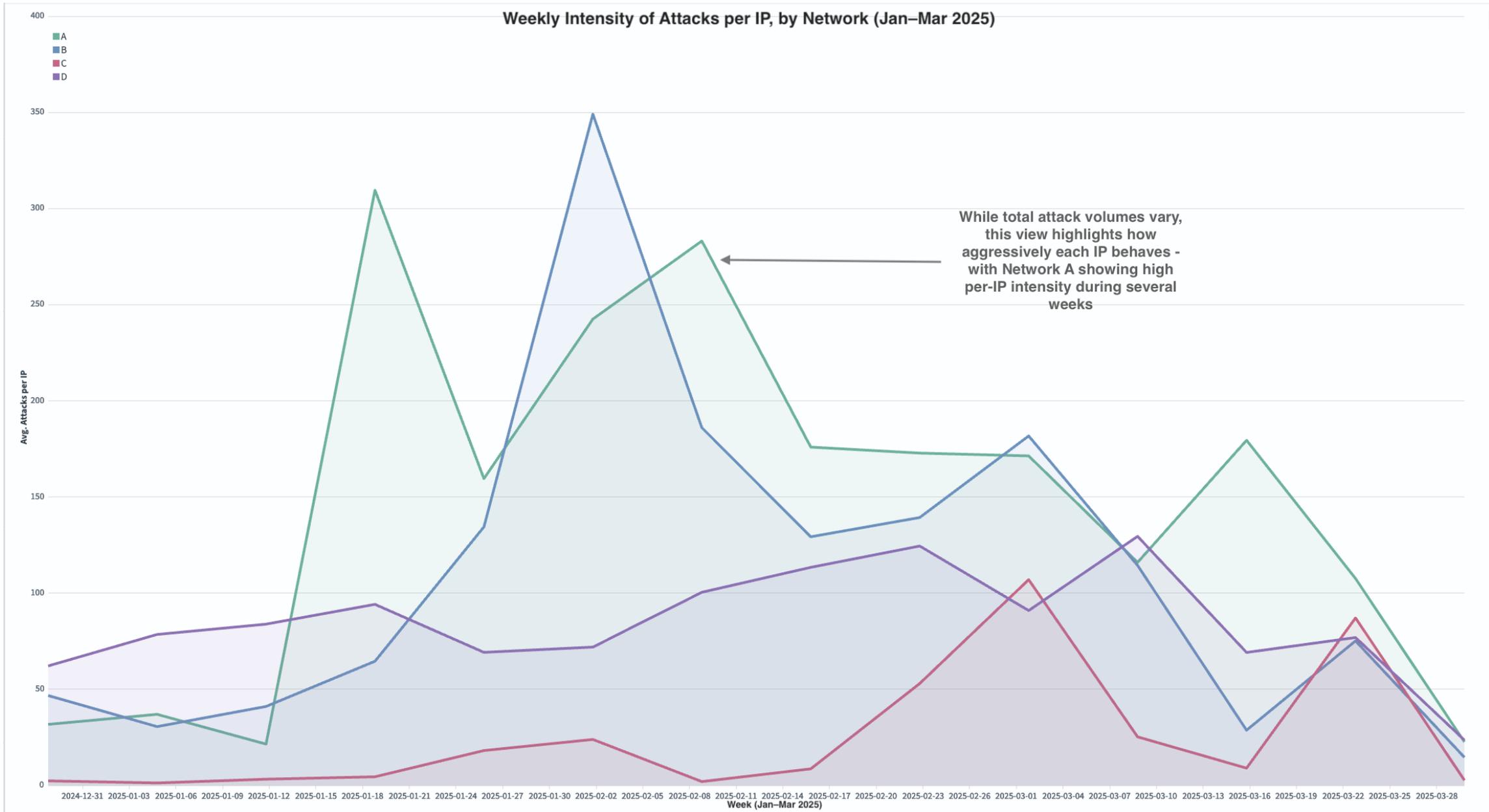- Success story: A collaborative approach to routing security

OUTLINE
STRENGTHENING INTERNET SECURITY

Relative Attack Volume by Network (Jan–Mar 2025)

While Network A showed high aggression per IP, Network D led in overall attack volume

FROM ORGANIZATIONS IN THIS ROOM – Q1 2025

Weekly Intensity of Attacks per IP, by Network (Jan–Mar 2025)

While total attack volumes vary, this view highlights how aggressively each IP behaves - with Network A showing high per-IP intensity during several weeks

FROM ORGANIZATIONS IN THIS ROOM – Q1 2025 WEEKLY

- ”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

Cloud-on-Cloud Activity: Attack Traffic Within the Same Hosting Network

Consistent intra-network attack traffic shows notable bursts
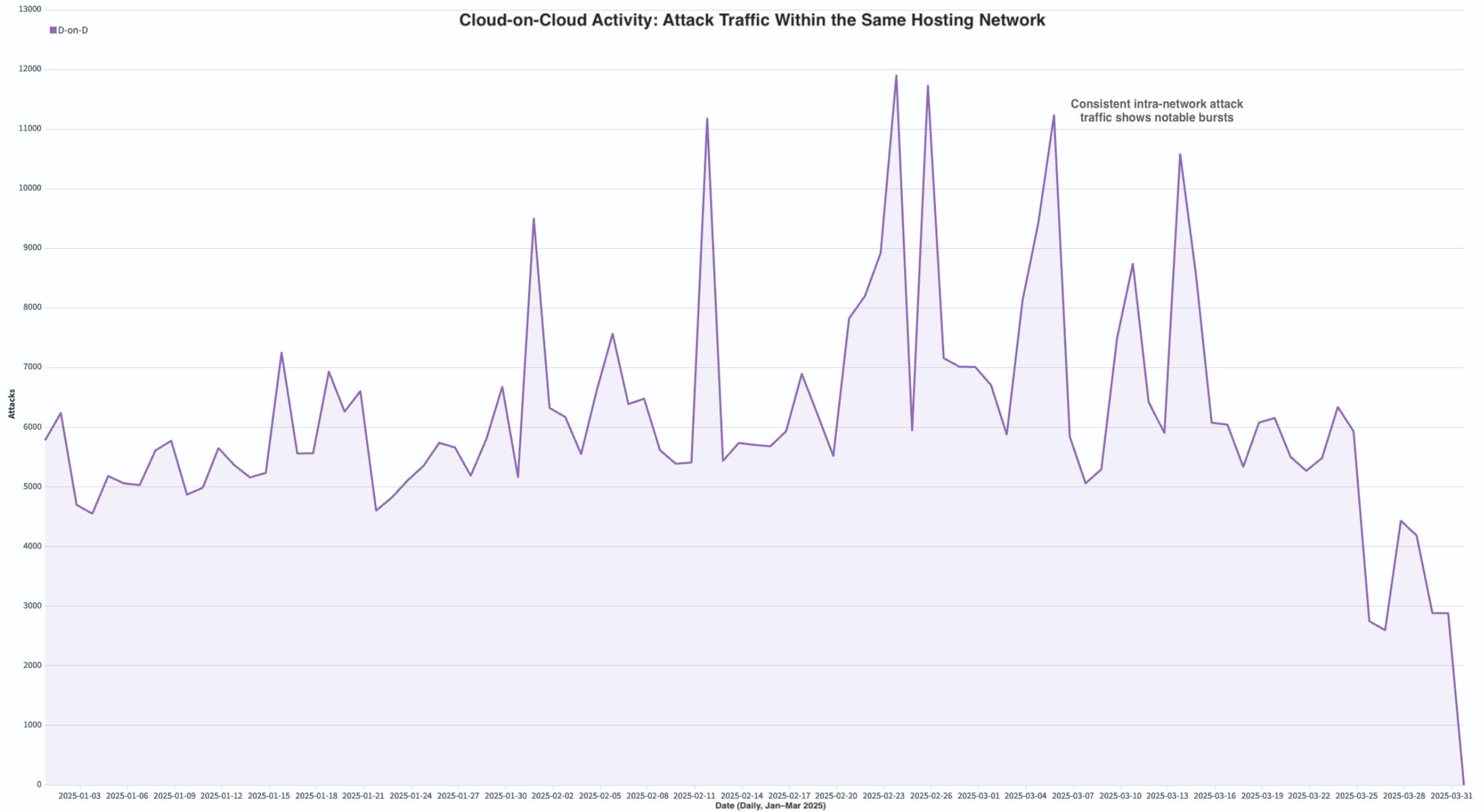
IT'S NOT IMPACTING YOUR CUSTOMERS... UNLESS IT IS

- Securing the Internet is
  - Hard
  - A collective action problem
  - Important

- Attack campaigns are playing out on the Internet
  - Small bot traffic
  - Big security impact
- We can see them.
  - Perhaps they can be stopped before they become multinational trans-network affairs?

- **Success story: A collaborative approach to routing security**

OUTLINE
STRENGTHENING INTERNET SECURITY

The Global Cyber Alliance's Internet Integrity Program **develops platforms** to provide insight for analysis of Internet cybersecurity threats and threat actors **and builds communities of Internet infrastructure operators** to identify and implement solutions

Mutually Agreed Norms for Routing Security (MANRS)

An undisputed minimum security baseline: the norm:

- *Defined through the* **MANRS Actions**
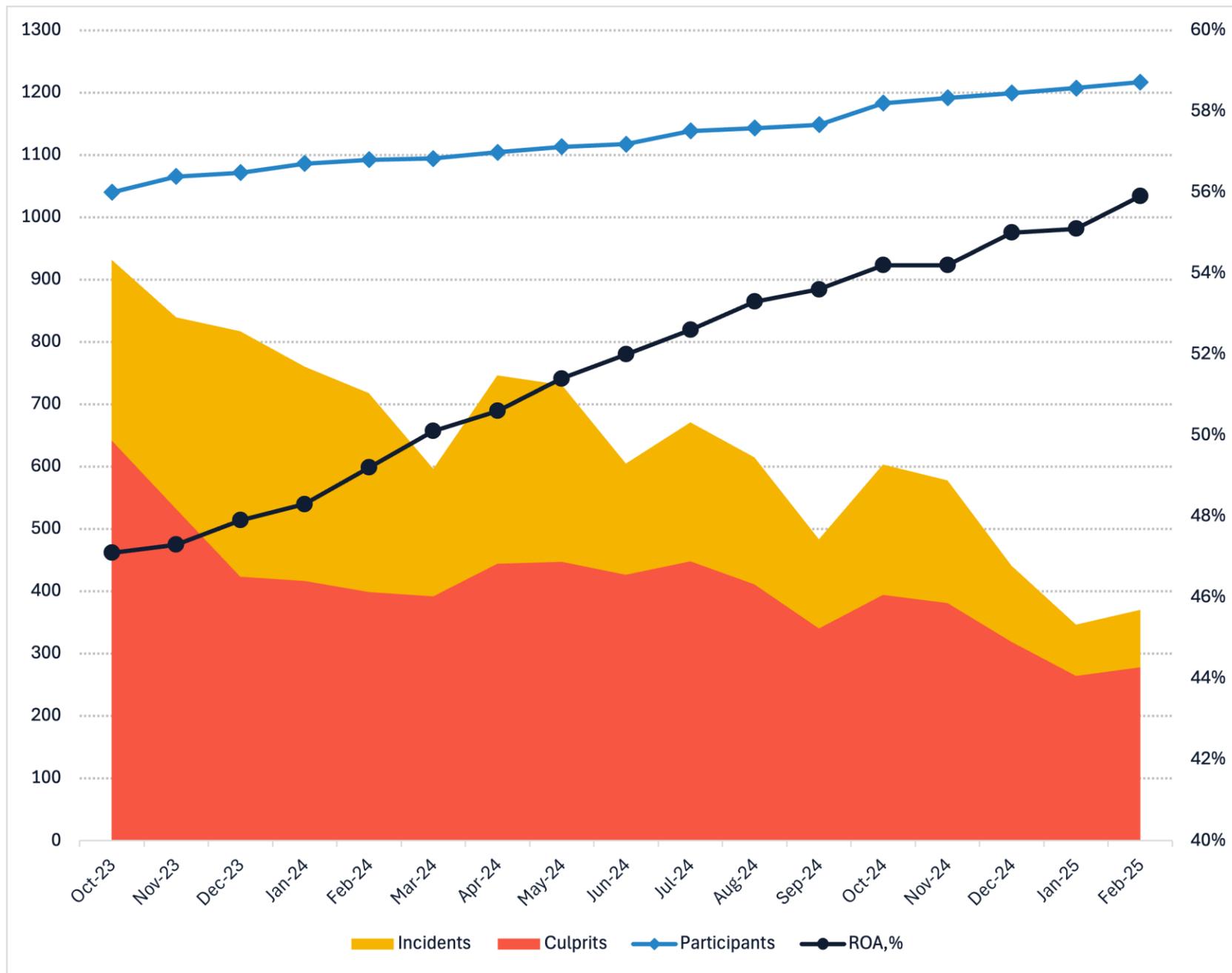
Demonstrated commitment by the participants:

- *Measured by the* **MANRS Observatory**

THE I2 PROGRAM
ANATOMY OF THE MANRS SUCCESS: THE PRINCIPLES

THE I2 PROGRAM

ANATOMY OF THE MANRS SUCCESS: THE IMPACT?

There are real threats out there in the Internet:

- *Some of them are **launching from your own networks***

You can help yourself by helping others (**collaboration**):

- *We have success stories*

The best solutions come from **industry consensus**:

- *We can help guide those discussions*
- *We can help promote outcomes*
- *We **CANNOT** determine the actions*

Collaboration over blocking every day

47

CONCLUSIONS AND TAKEAWAYS

THANK YOU!

ldaigle@globalcyberalliance.org

GLOBAL
CYBER
ALLIANCE.