

STRENGTHENING INTERNET SECURITY

COLLABORATIVE SOLUTIONS FOR CYBERSECURITY CHALLENGES

LESLIE DAIGLE, GLOBAL CYBER ALLIANCE

September 9, 2025. Da Nang -- APNIC60






REMEMBER?

- 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

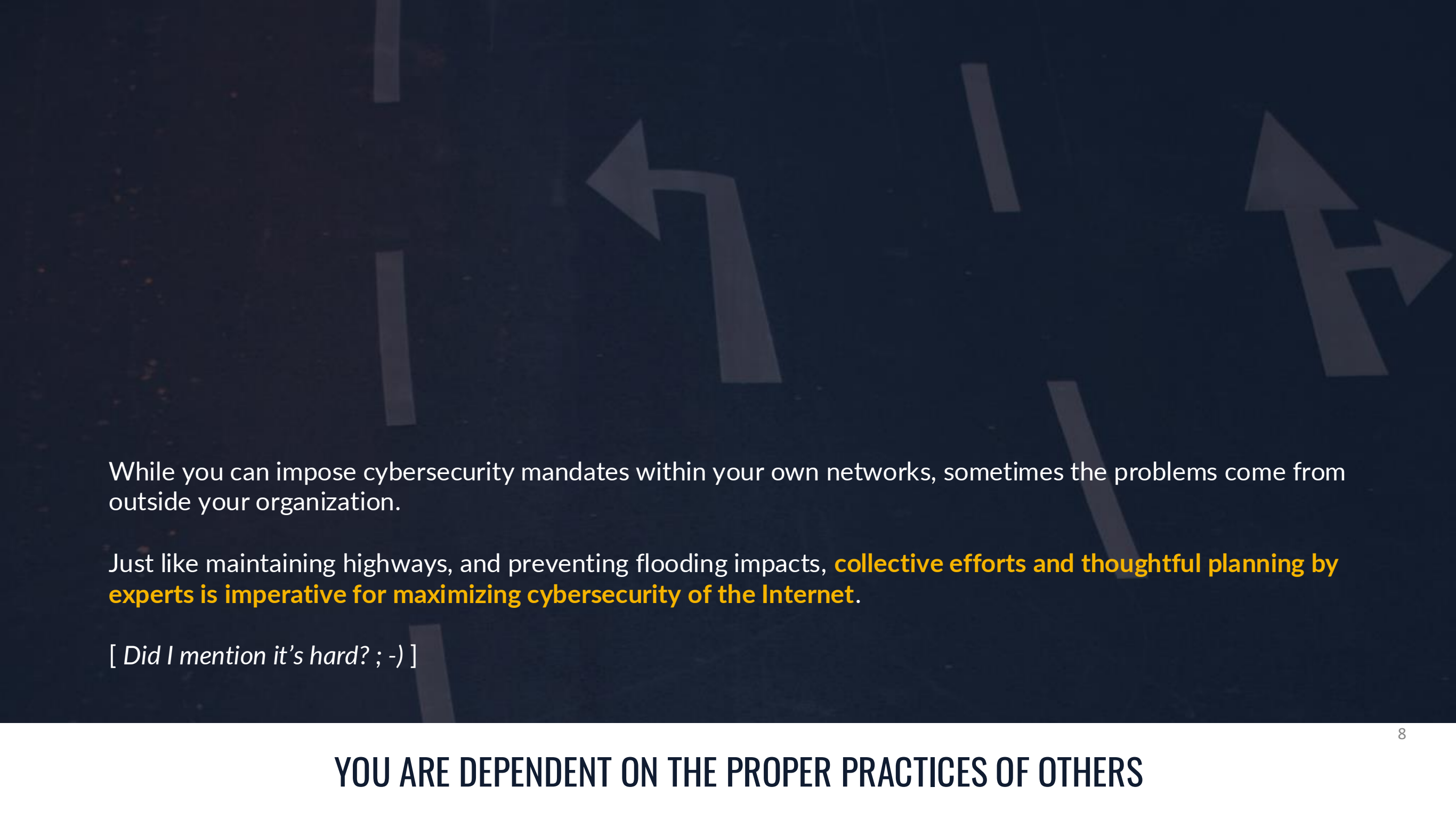
OUTLINE

STRENGTHENING INTERNET SECURITY

- The Internet defined this concept, before there was an award-winning 2022 movie ;)
- In order to be able to sit in Da Nang 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

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

- UnitedHealth Group said its quarterly earnings fell **BY MORE THAN A FIFTH** after a cyberattack in February 2024 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.**

WHY WE (ALL) CARE ABOUT SECURING THE INTERNET?

Little things can lead to big threats

- **APT36:** Demonstrates weaponization of ISP infrastructure for nation-state espionage amid India–Pakistan tensions.
- **RedTail:** Highlights critical risk to Asia-Pacific economies' compute and financial infrastructure—malicious resource theft can degrade service availability and fund further nation-state cyber operations.
- **Kimsuky:** Exposes vulnerabilities in soft targets—especially academic and policy institutions—across South Korea, Japan, and Southeast Asia.
- **Dark Pink:** Attribution suggests possible link to OceanLotus or other Southeast Asia-based actors.

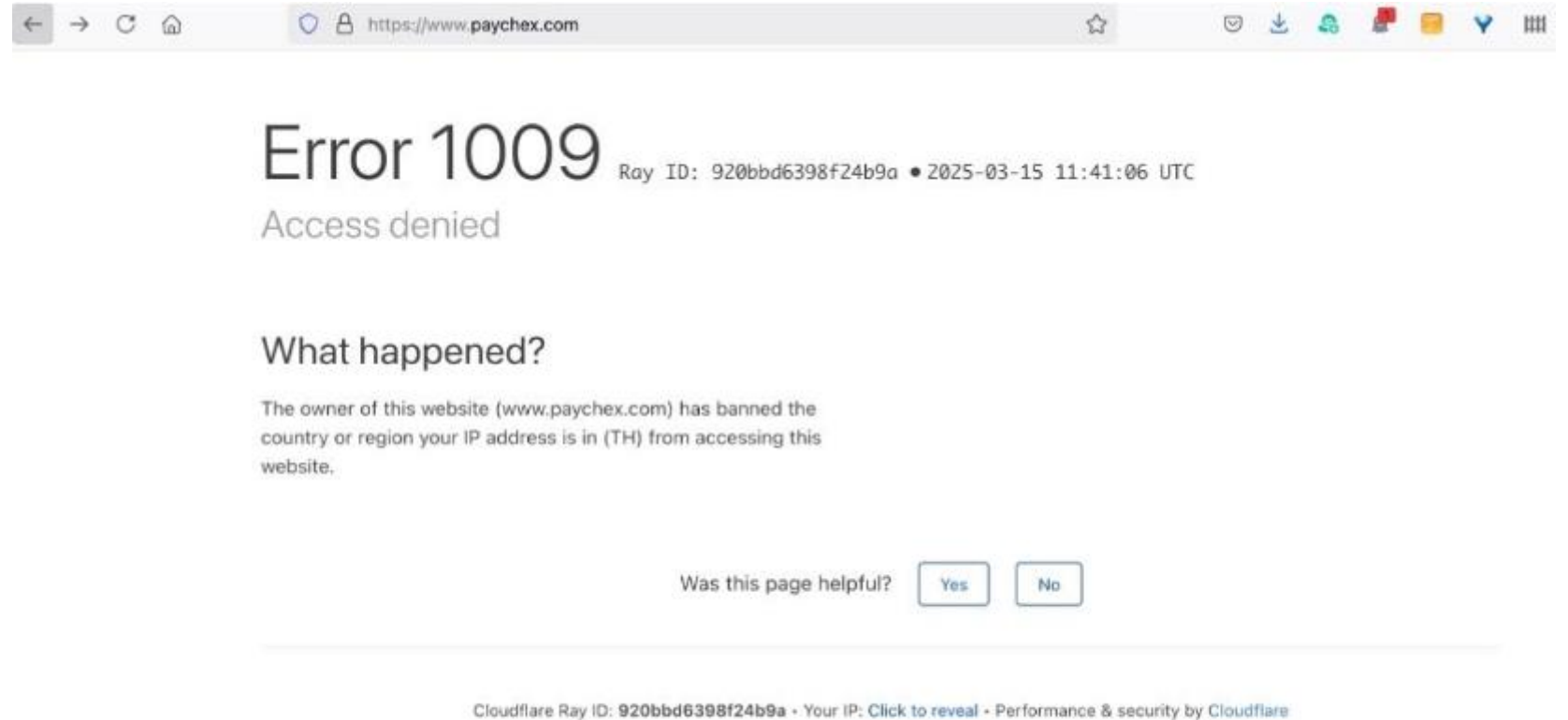
INTERNET INTEGRITY

CONCRETELY: WHY IT MATTERS?



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?*



WHAT IT LOOKS LIKE WHEN WE GET IT WRONG?

The background is a dense, overlapping collage of torn pieces of paper. The paper features various patterns, including geometric shapes, floral motifs, and abstract designs. The color palette is primarily blue, yellow, and white, with some darker blue and red accents. The edges of the paper are ragged and torn, creating a textured, layered effect. Overlaid on this collage is the text "SO, THEN, WHAT?" in a bold, yellow, sans-serif font. The text is centered horizontally and vertically, with a slight shadow or transparency effect that makes it stand out against the busy background.

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*



INTERNET INTEGRITY

NAMES, NUMBERS, AND ROUTES



INTERNET INTEGRITY
NAMES, NUMBERS, AND ROUTES

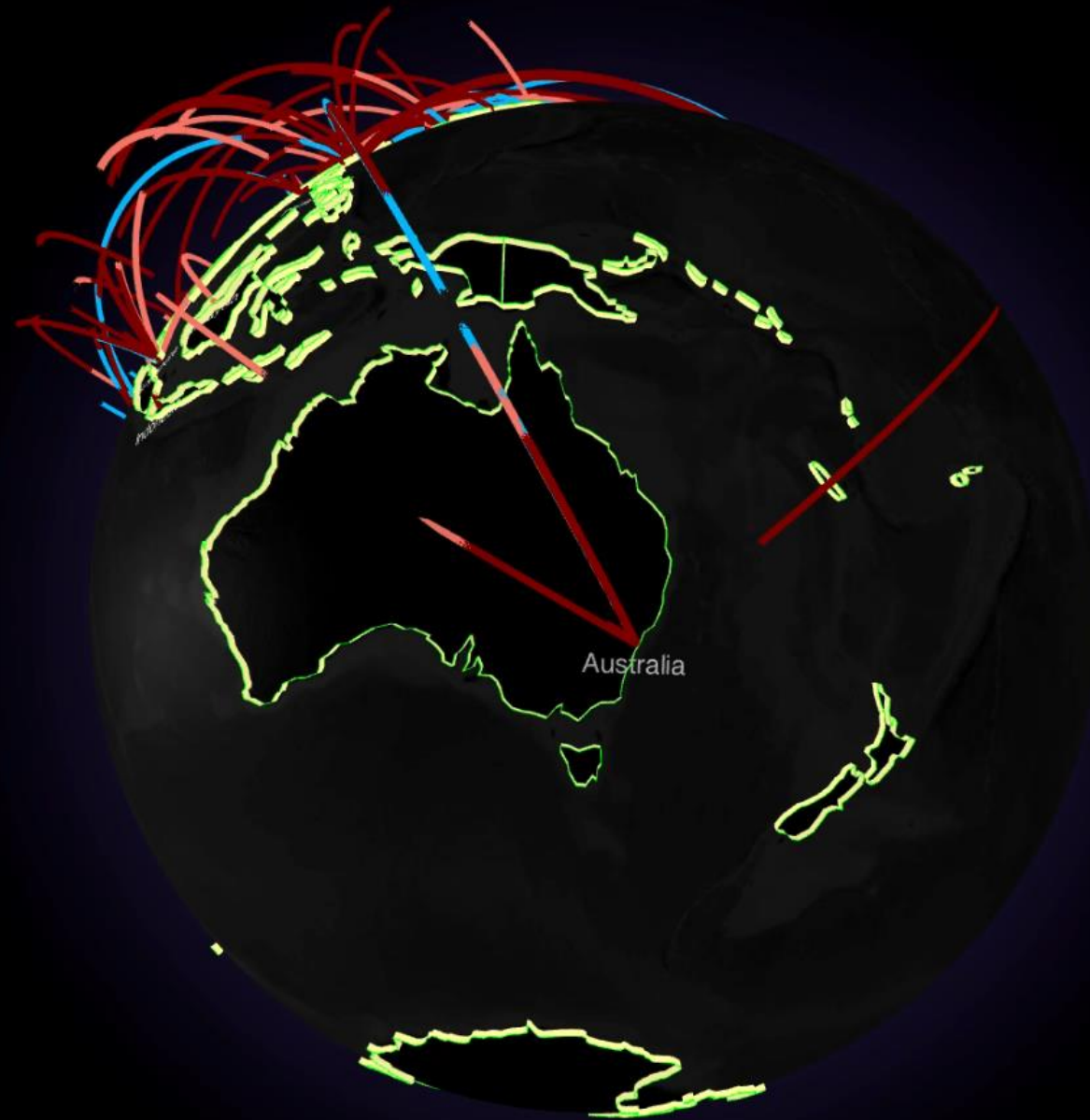
- Securing the Internet is
 - Hard
 - A collective action problem
 - Important
- **Attack campaigns are playing out on the Internet**
 - **Small bot traffic**
 - Big security impact
- We can see them.
 - Perhaps they can be stopped before they become multinational trans-network affairs?
- Success story: A collaborative approach to routing security

OUTLINE

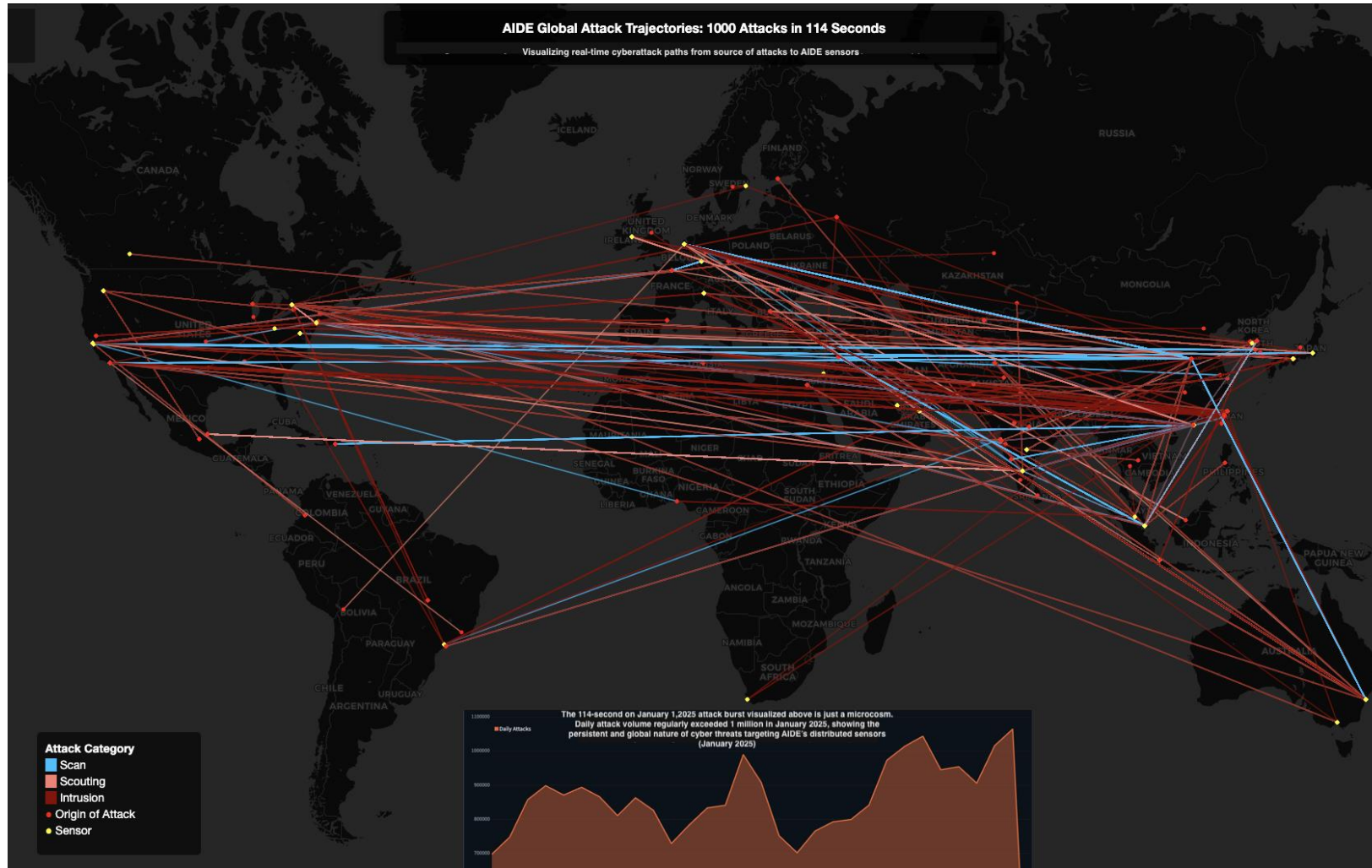
STRENGTHENING INTERNET SECURITY



ATTACKS BY THE NUMBERS



- Scan
- Scouting
- Intrusion



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

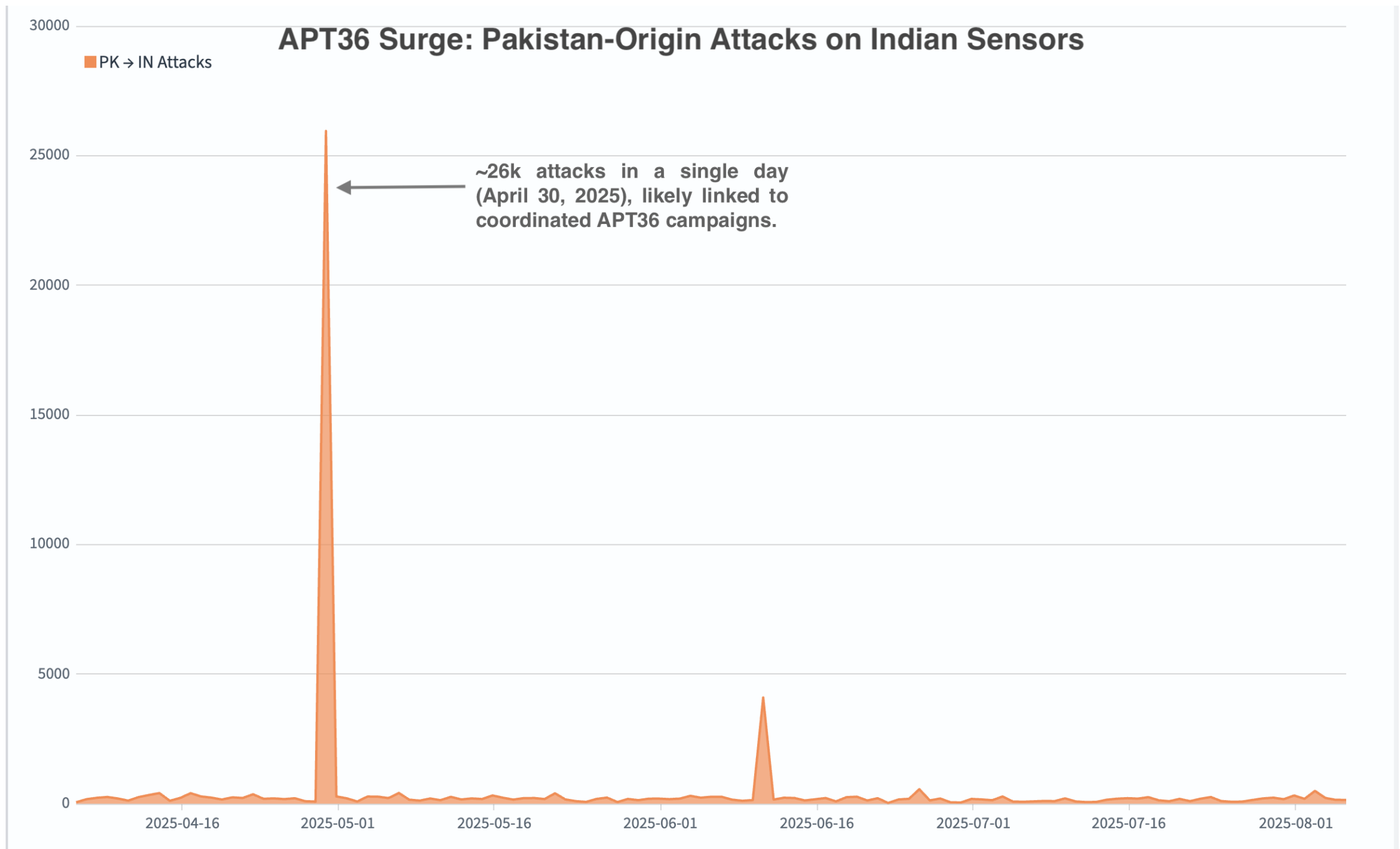
OUTLINE

STRENGTHENING INTERNET SECURITY

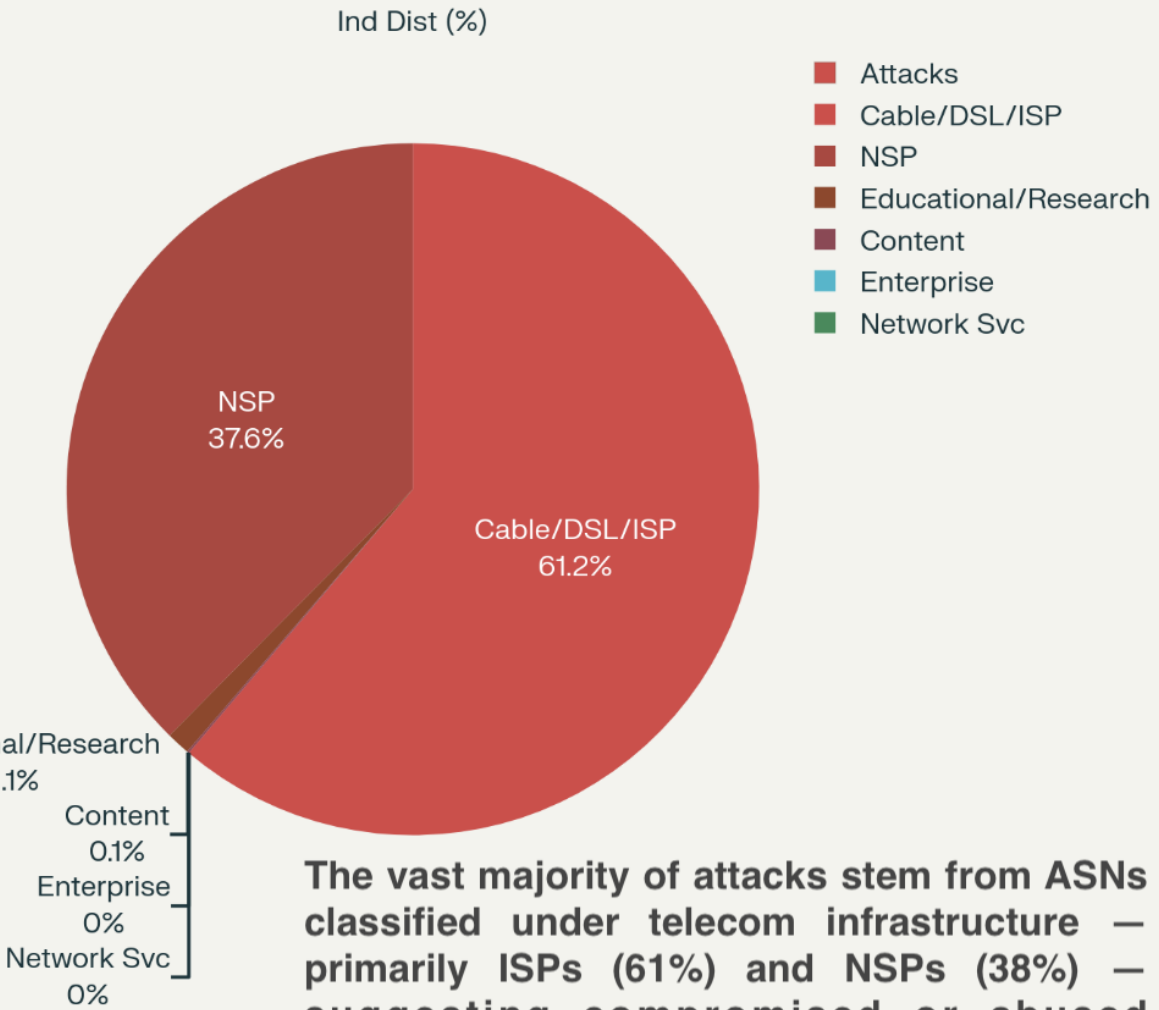
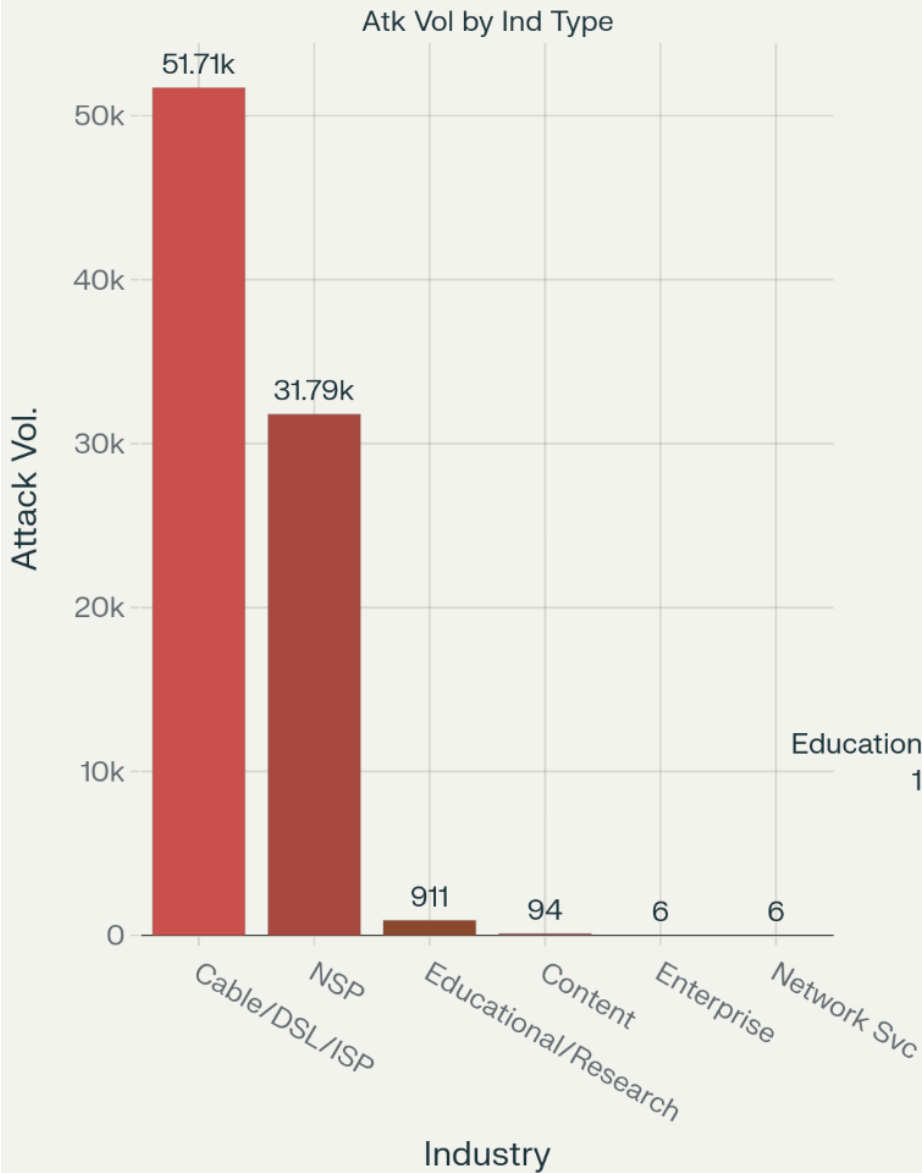
- Type: Geopolitical
- Activity: Persistent phishing, credential harvesting, and malware deployment against Indian military and government sectors.
- Why does it matter: Demonstrates weaponization of ISP infrastructure for nation-state espionage amid India–Pakistan tensions

BIG IMPACT – APT36

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



APT36 Attack Origins by ASN Industry



The vast majority of attacks stem from ASNs classified under telecom infrastructure — primarily ISPs (61%) and NSPs (38%) — suggesting compromised or abused backbone providers are a key enabler in APT36 operations.

- Type: Financially Motivated
- Activity: Cryptomining campaign with Lazarus-linked infrastructure targeting finance-heavy regions.
- Why It Matters: Highlights critical risk to Asia Pacific economies' compute and financial infrastructure—malicious resource theft can degrade service availability and fund further nation-state cyber operations.

BIG IMPACT – RedTail

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

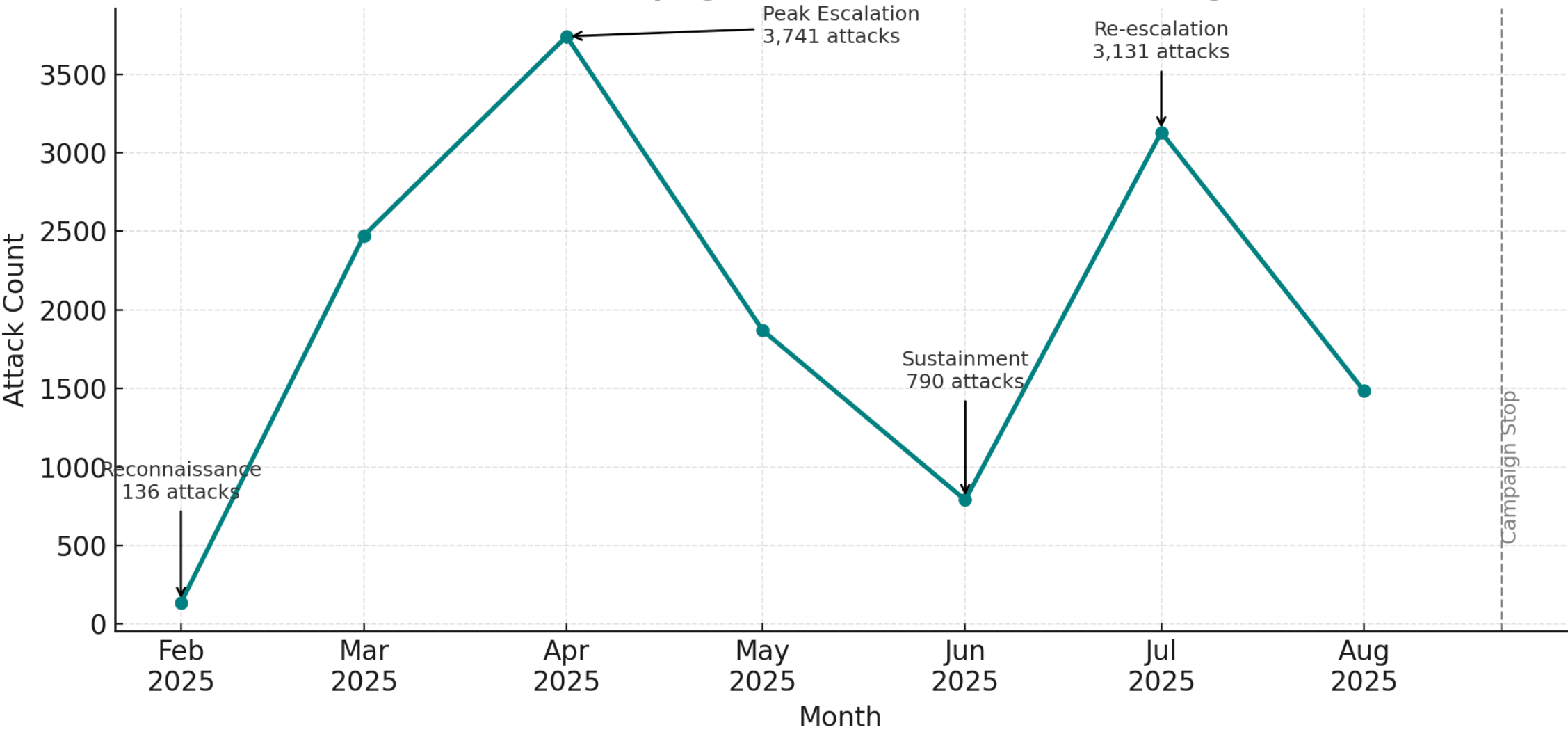
RedTail Malware Attack Flows: Targeting Asia-Pacific

● Source Countries ● Target Countries — Attack Flows

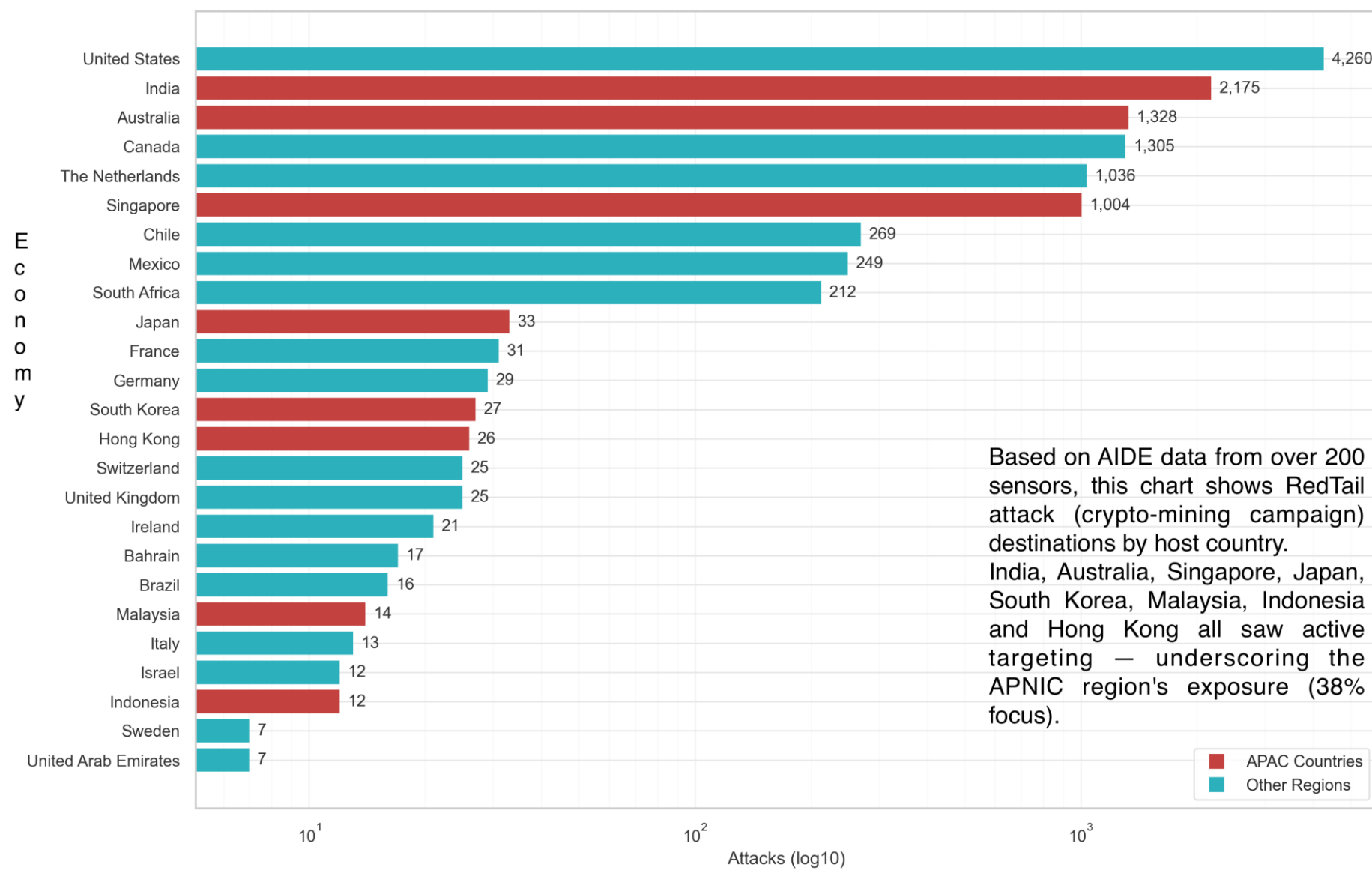


Traffic is funneled through infrastructure in Europe and offshore regions—suggesting proxy use—to reach 74% of APAC targets.

RedTail Attack Campaign Phases in Asia-Pacific (Feb-Aug 2025)



RedTail Activity Observed by AIDE Sensors - Top Targeted Economies

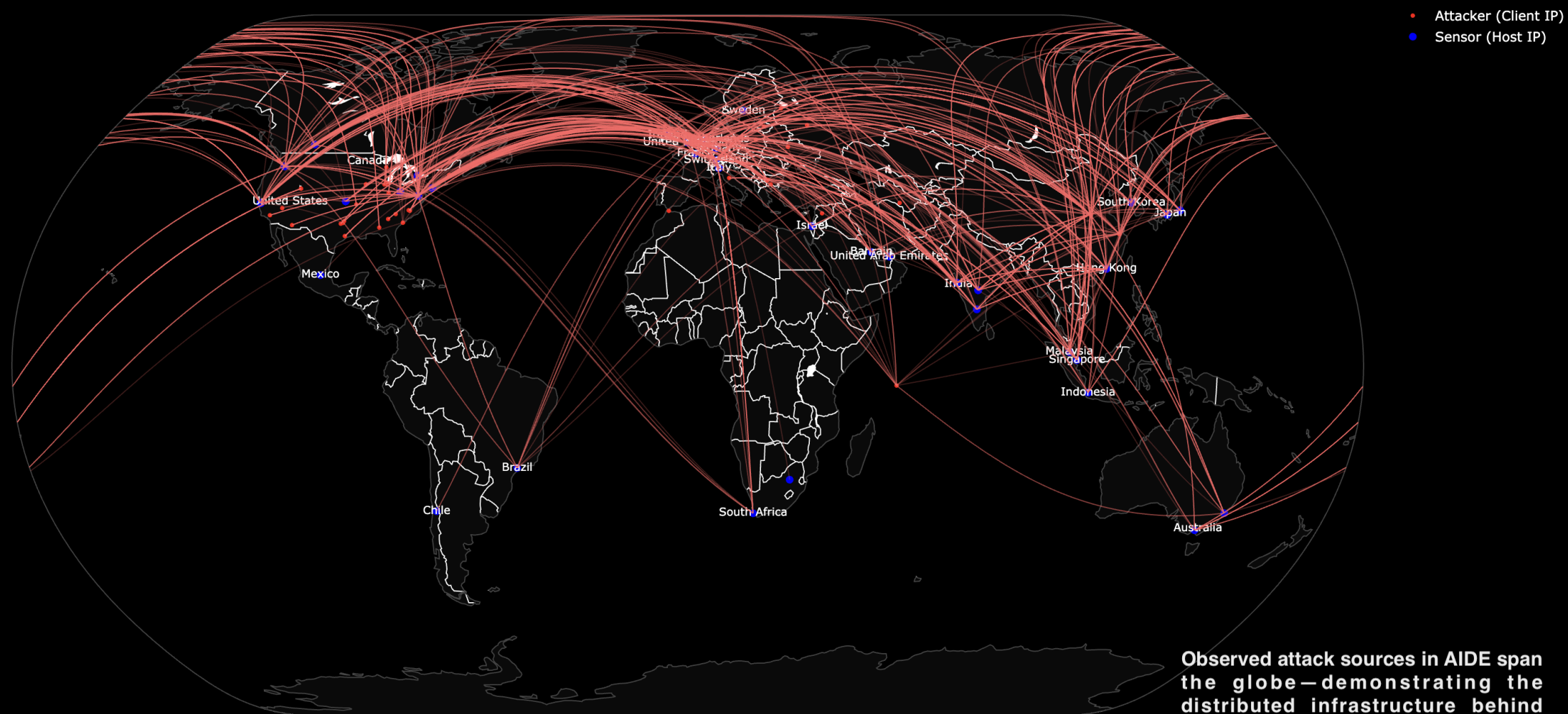


- Type: Espionage
- Activity: Remote access trojans and phishing infrastructure aimed at researchers, diplomats, and think tanks.
- Why It Matters: Exposes vulnerabilities in soft targets—especially academic and policy institutions—across South Korea, Japan, and Southeast Asia.

BIG IMPACT – Kimsuky

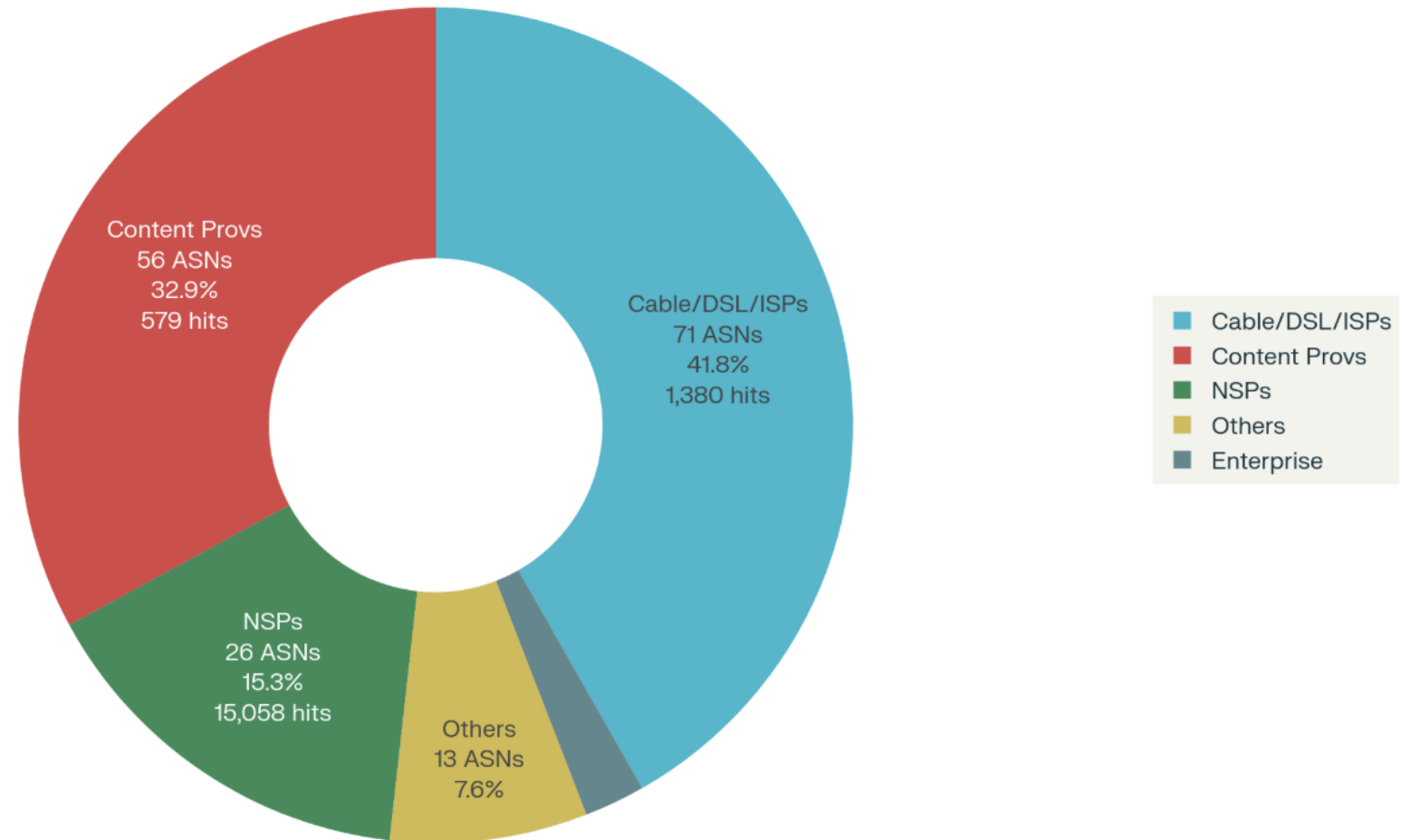
THEY'RE NOT JUST BEING FRIENDLY AND SAYING "HELLO"

AIDE Reveals Global Reach of Suspicious Kimsuky Activity

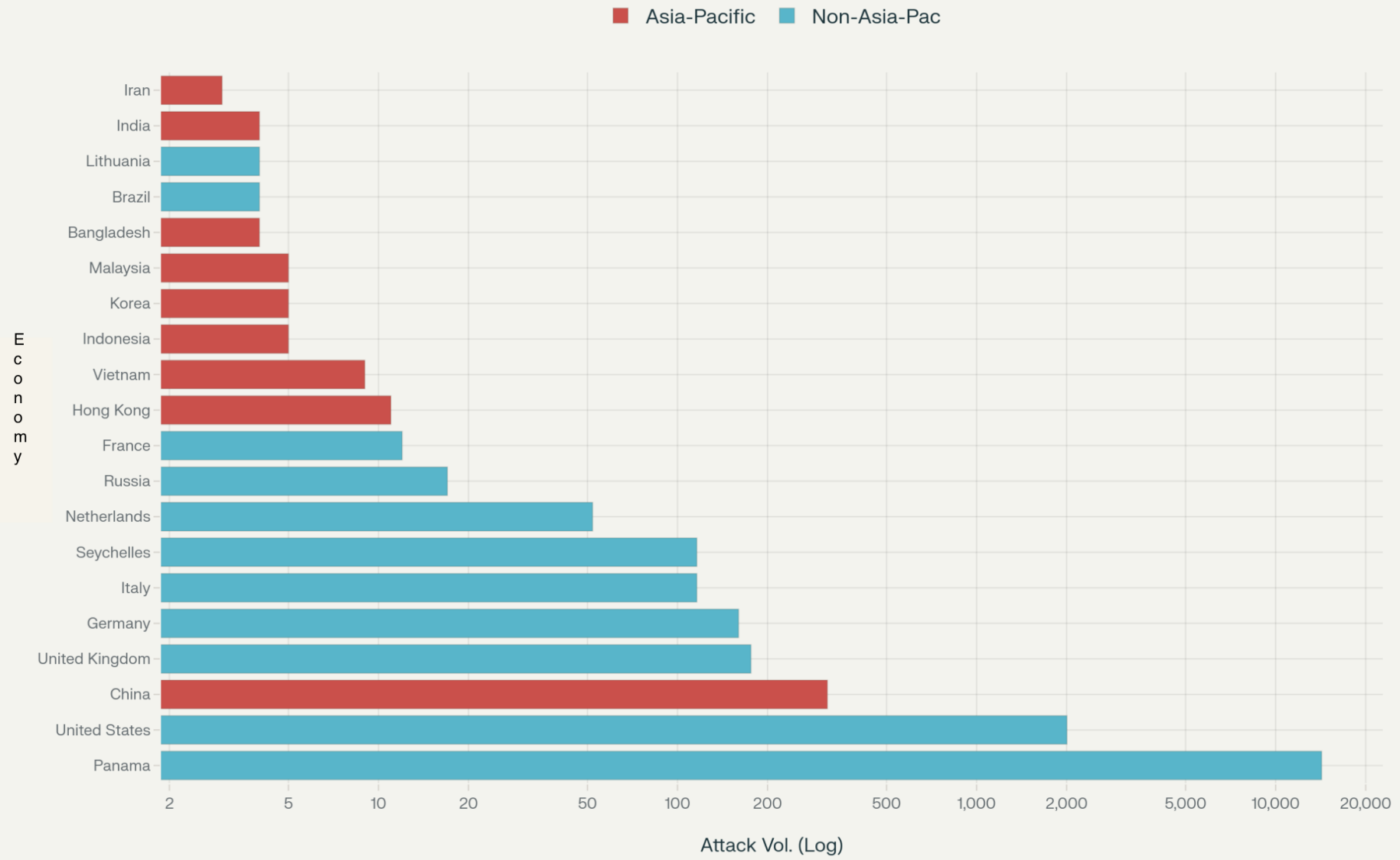


Observed attack sources in AIDE span the globe—demonstrating the distributed infrastructure behind Kimsuky (N. Korea-linked) activity.

Kimsuky ASN Industry Distribution

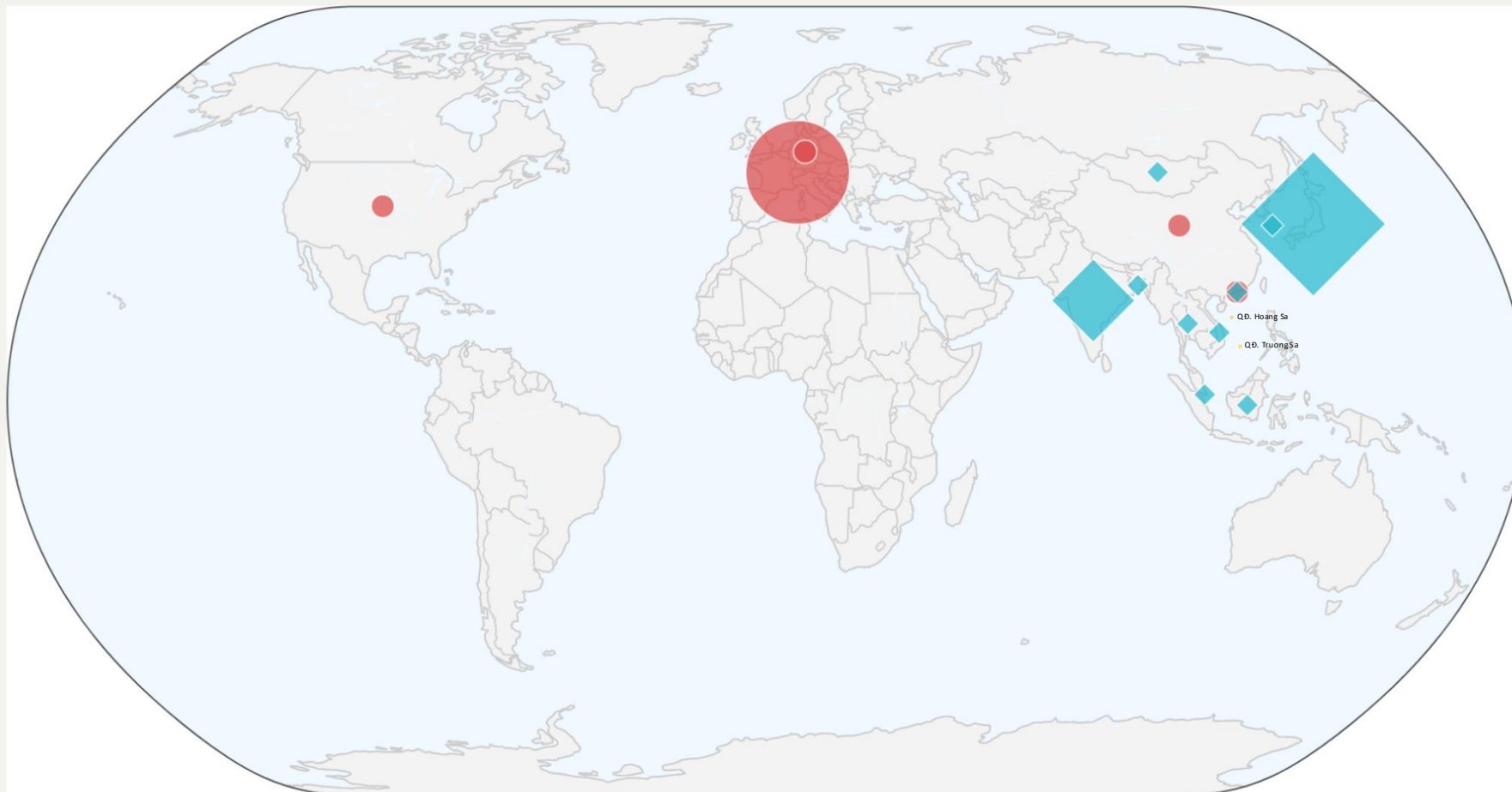


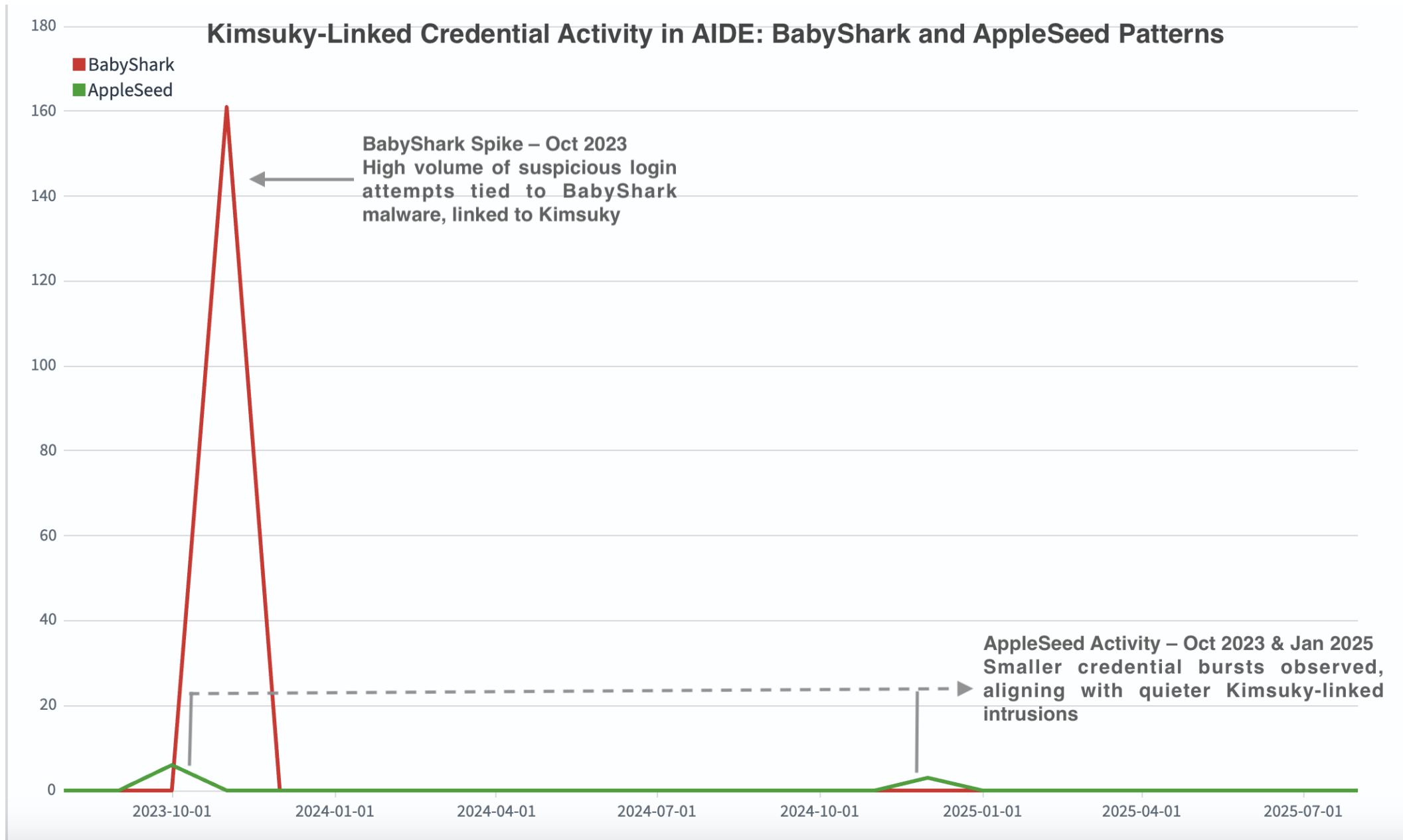
Kimsuky Attacks by Economies (Log Scale)

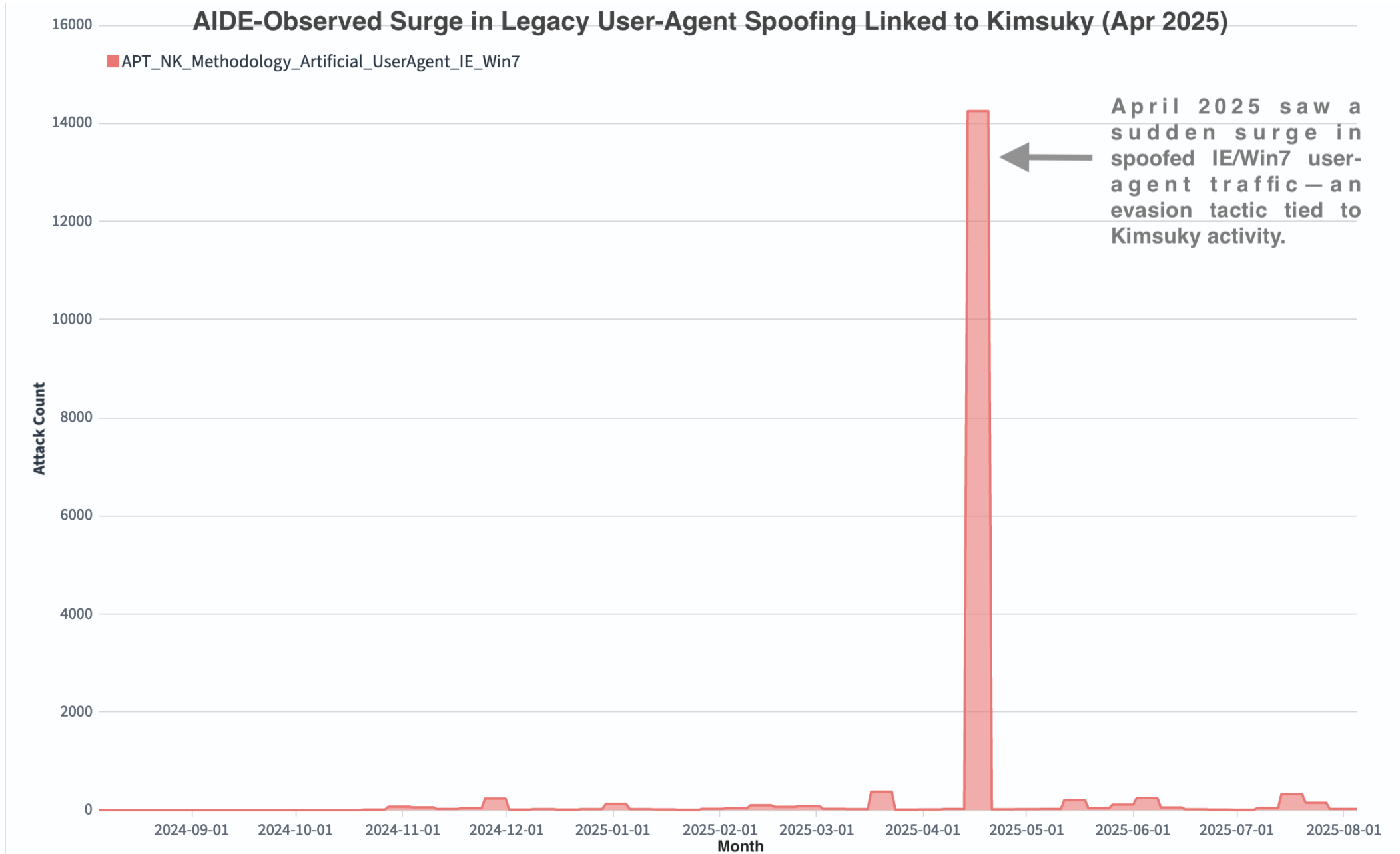


Kimsuky: Global Attacking Sources vs APAC AIDE Targets

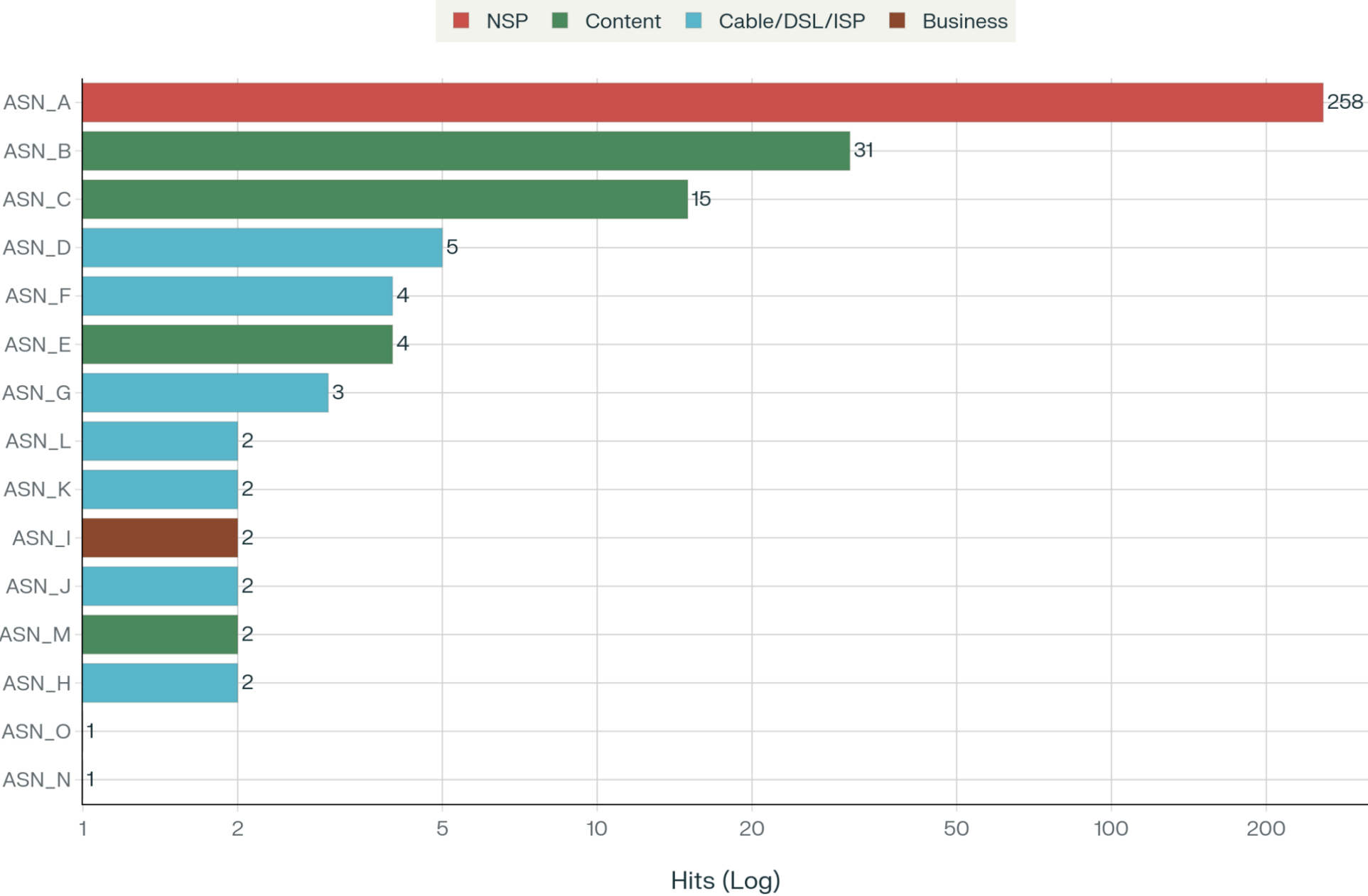
● Attack Sources ◆ AIDE Sensors in APAC







Top 15 APAC ASNs by Kimsuky



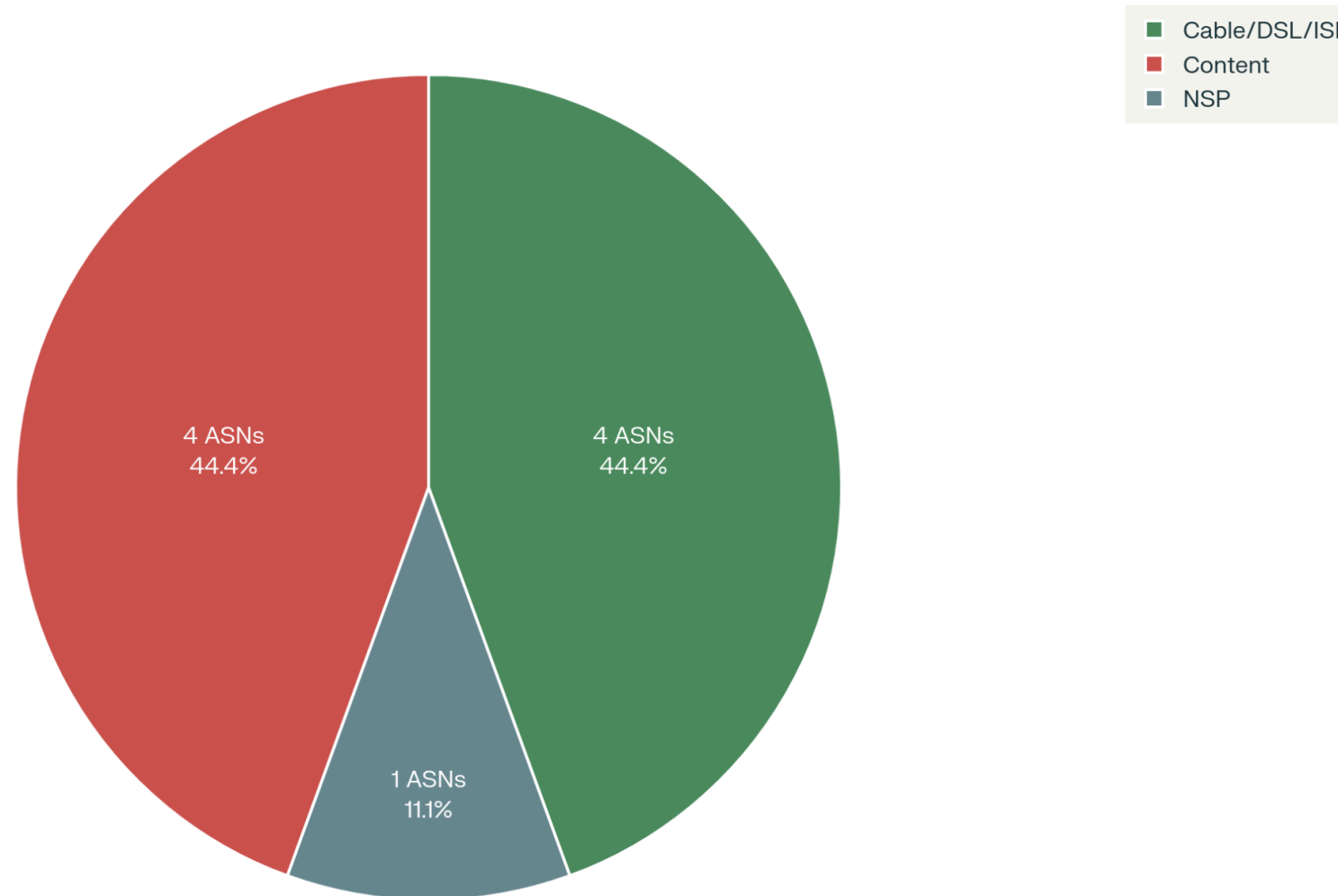
- Type: Strategic Access & Information Operations
- Activity: Observed using DLL sideloading and command-and-control techniques to target military and government orgs in Indonesia, the Philippines, and Malaysia.
- Why It Matters: Attribution suggests possible link to OceanLotus or other Southeast Asia-based actors.

BIG IMPACT – Dark Pink

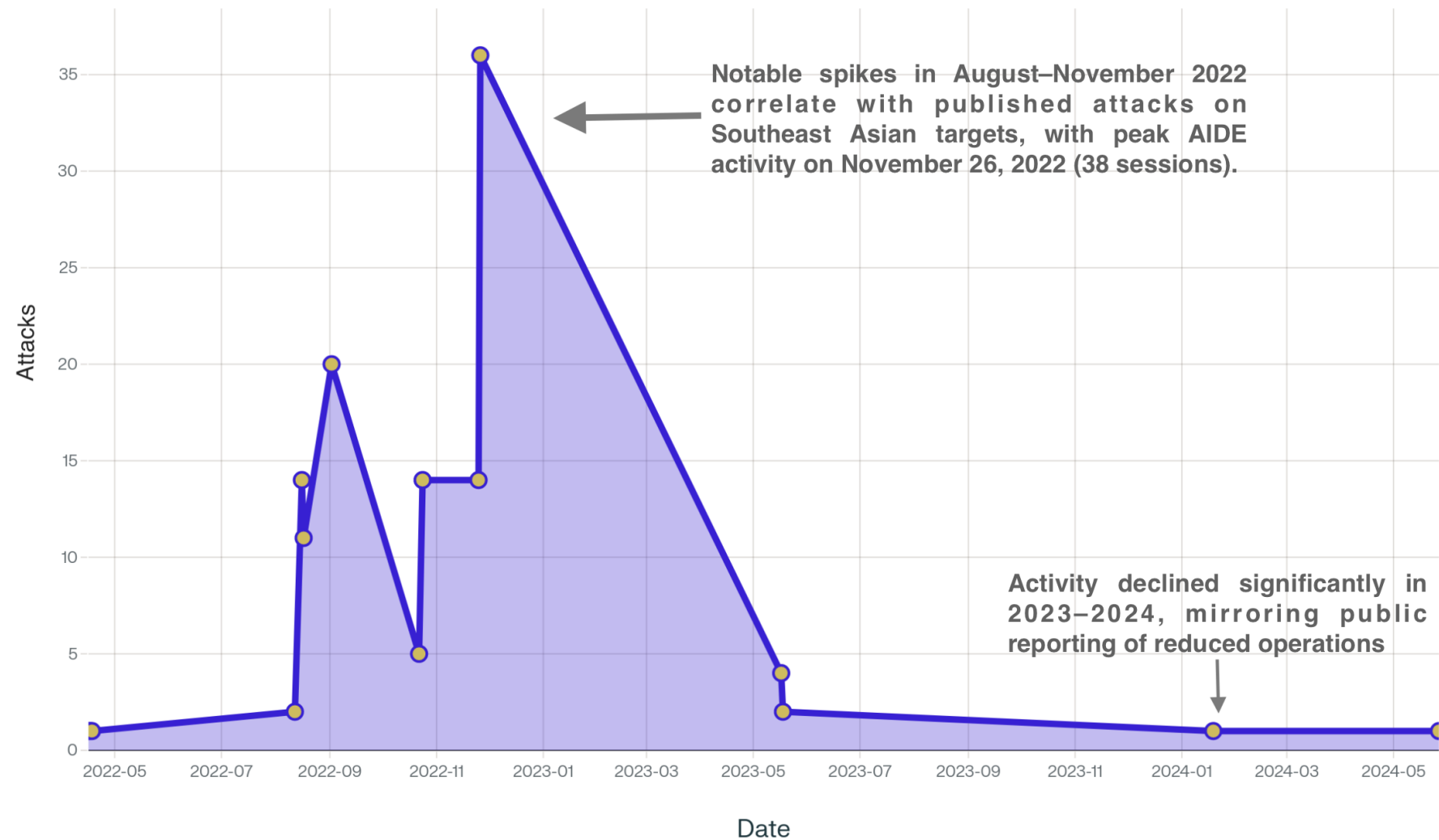
THEY'RE NOT JUST BEING FRIENDLY AND SAYING "HELLO"

Dark Pink APT – ASN Distribution by Industry Type

Majority of infrastructure traced to Content and Cable/DSL/ISP providers

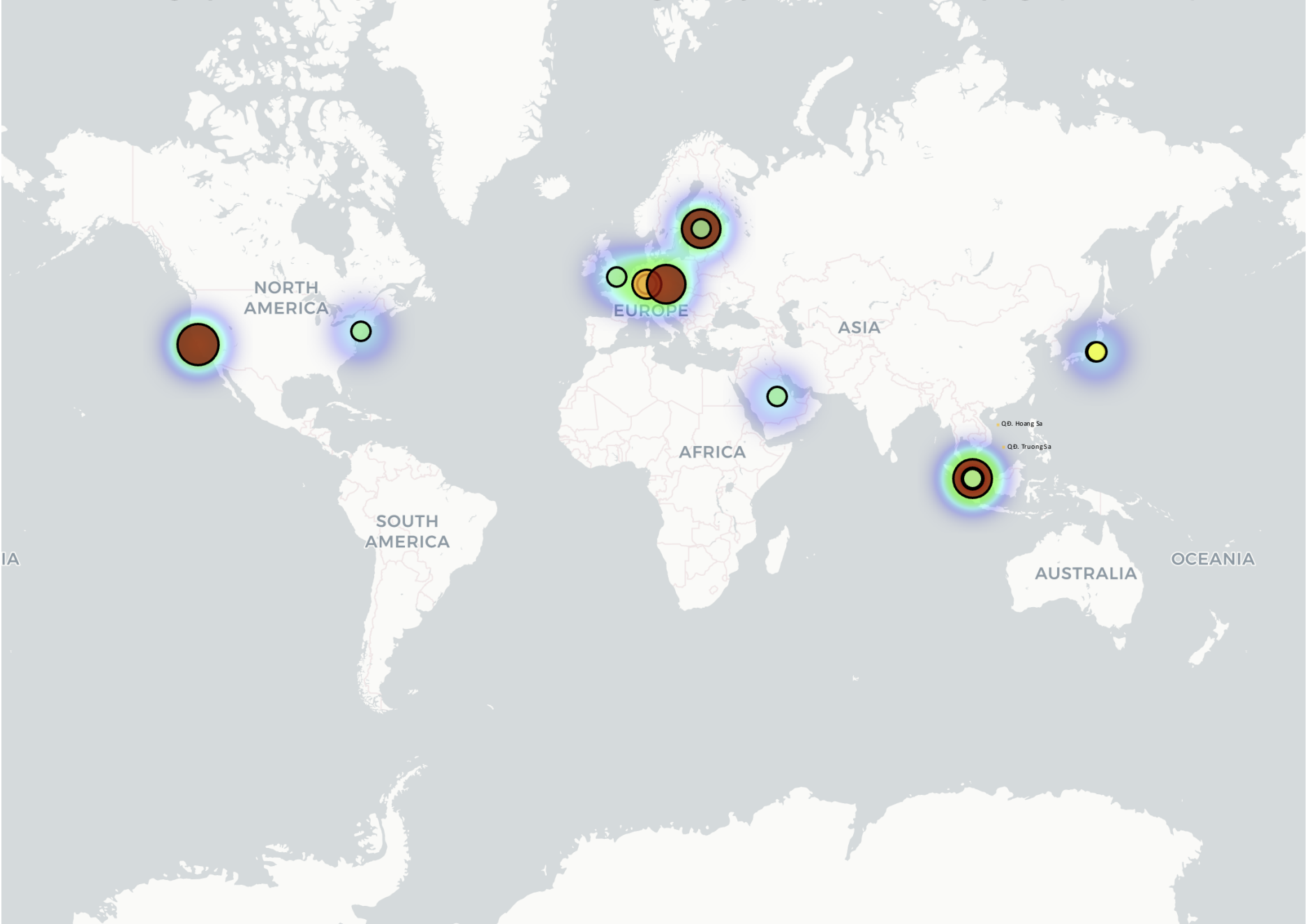


Dark Pink APT – Timeline of Activity Observed in AIDE Sensors

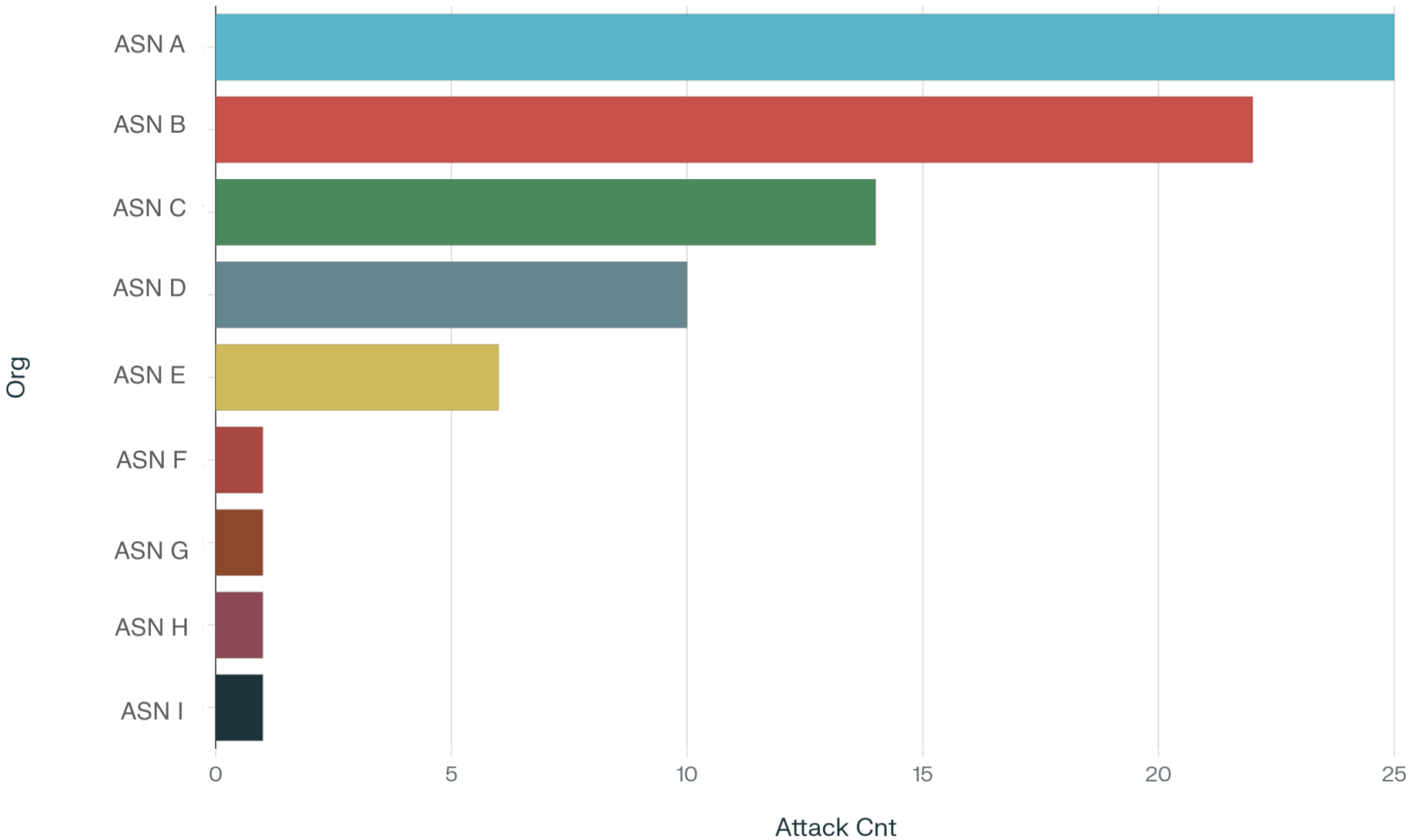


Dark Pink APT: Global Footprint of Attacks Observed in AIDE (Southeast Asia Attribution)

Geographic heatmap of sensor locations targeted by the Dark Pink campaign (2022–2024)



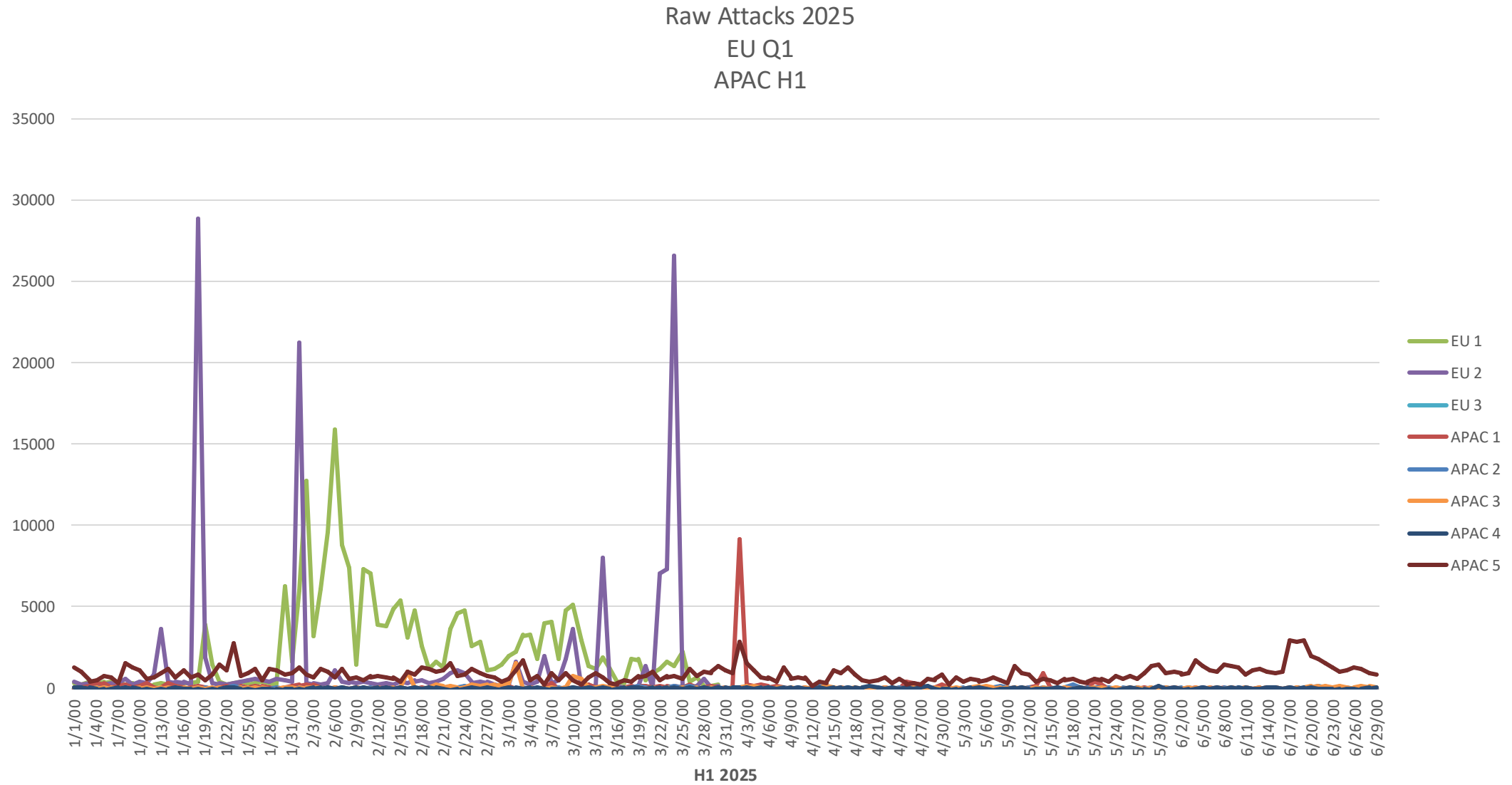
Dark Pink Campaign – Source ASNs Behind Attacks (Observed in AIDE Sensors)



- 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

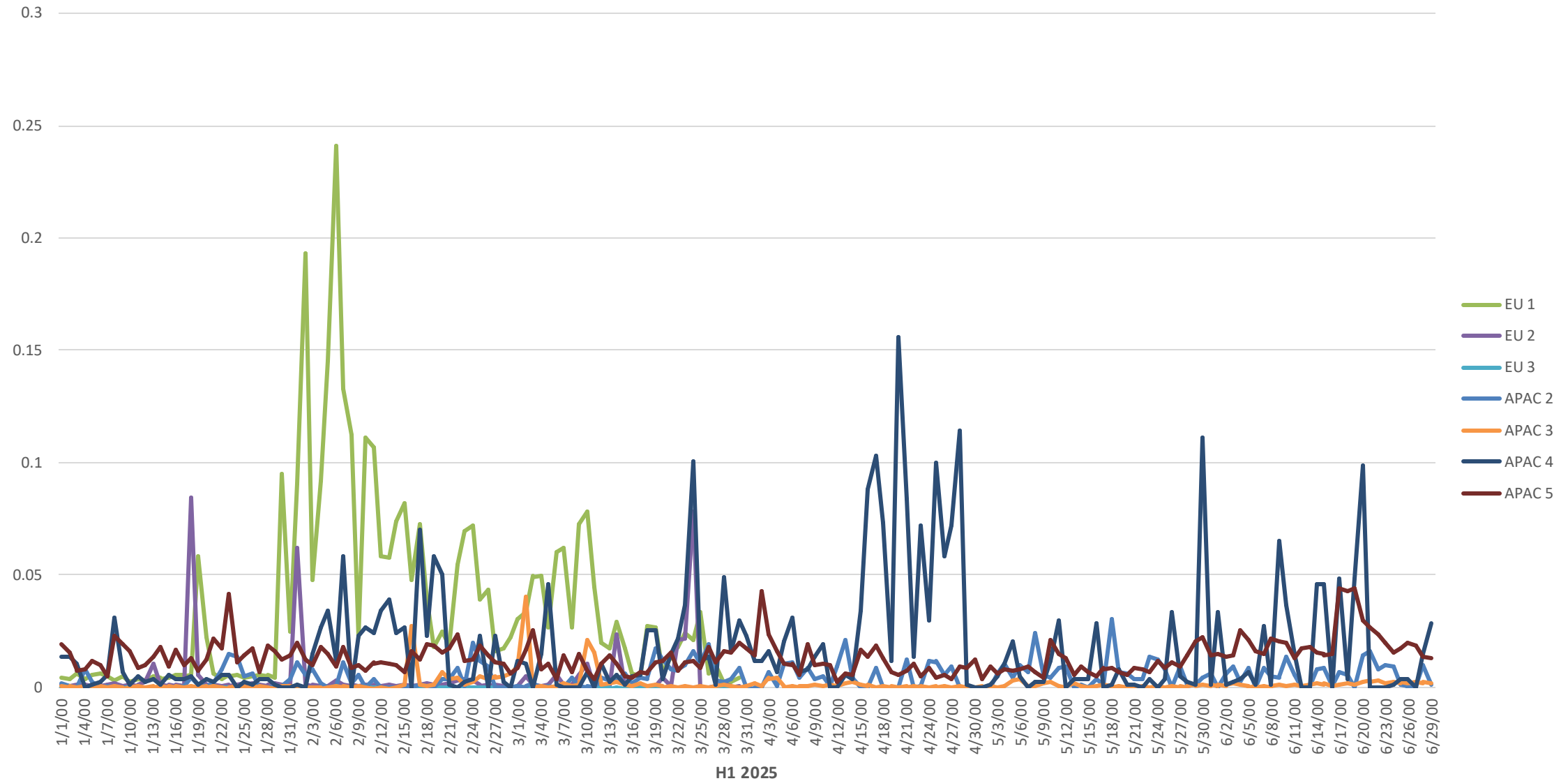
OUTLINE

STRENGTHENING INTERNET SECURITY

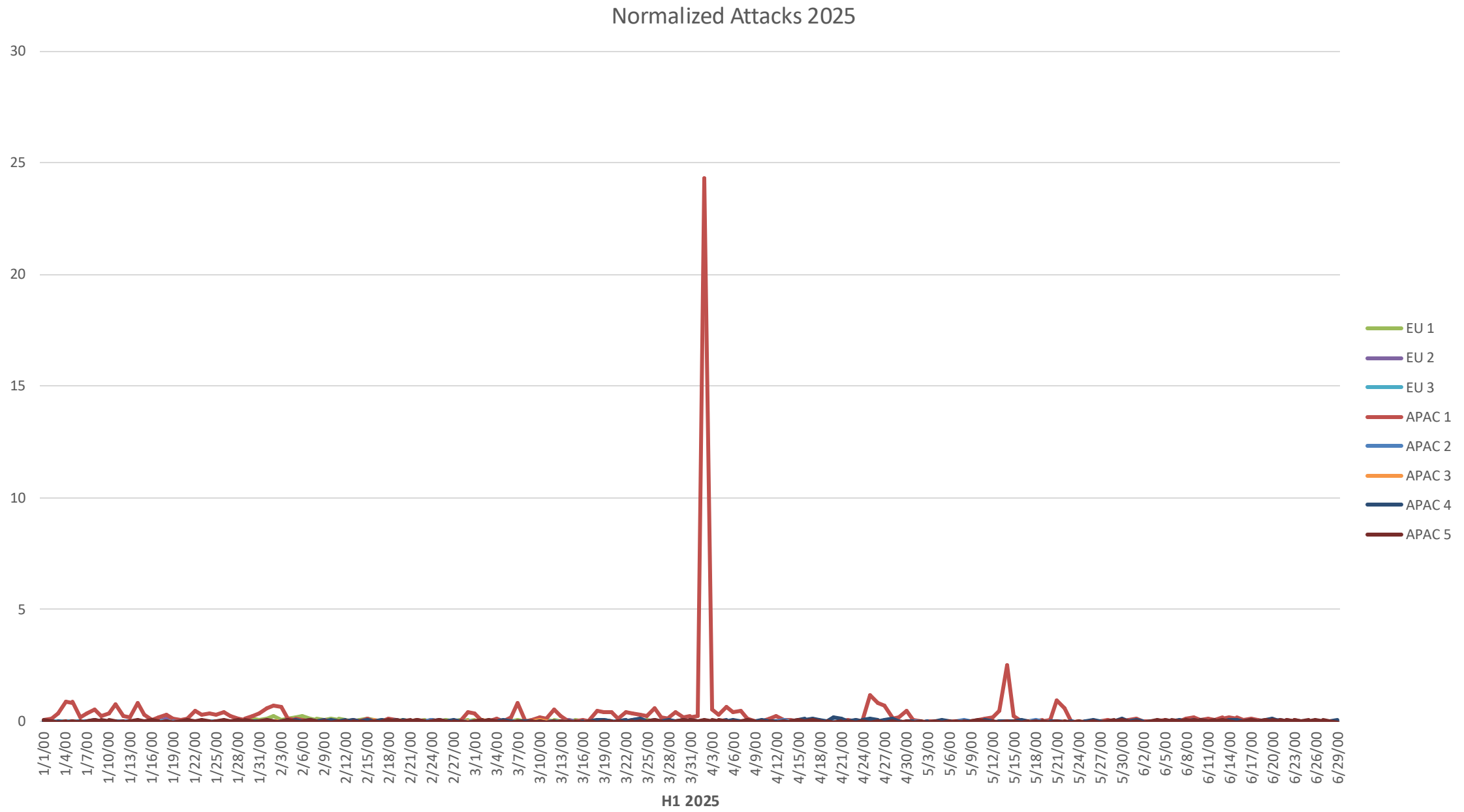


INCLUDING ORGANIZATIONS IN THIS ROOM – H1 2025

Normalized Attacks 2025



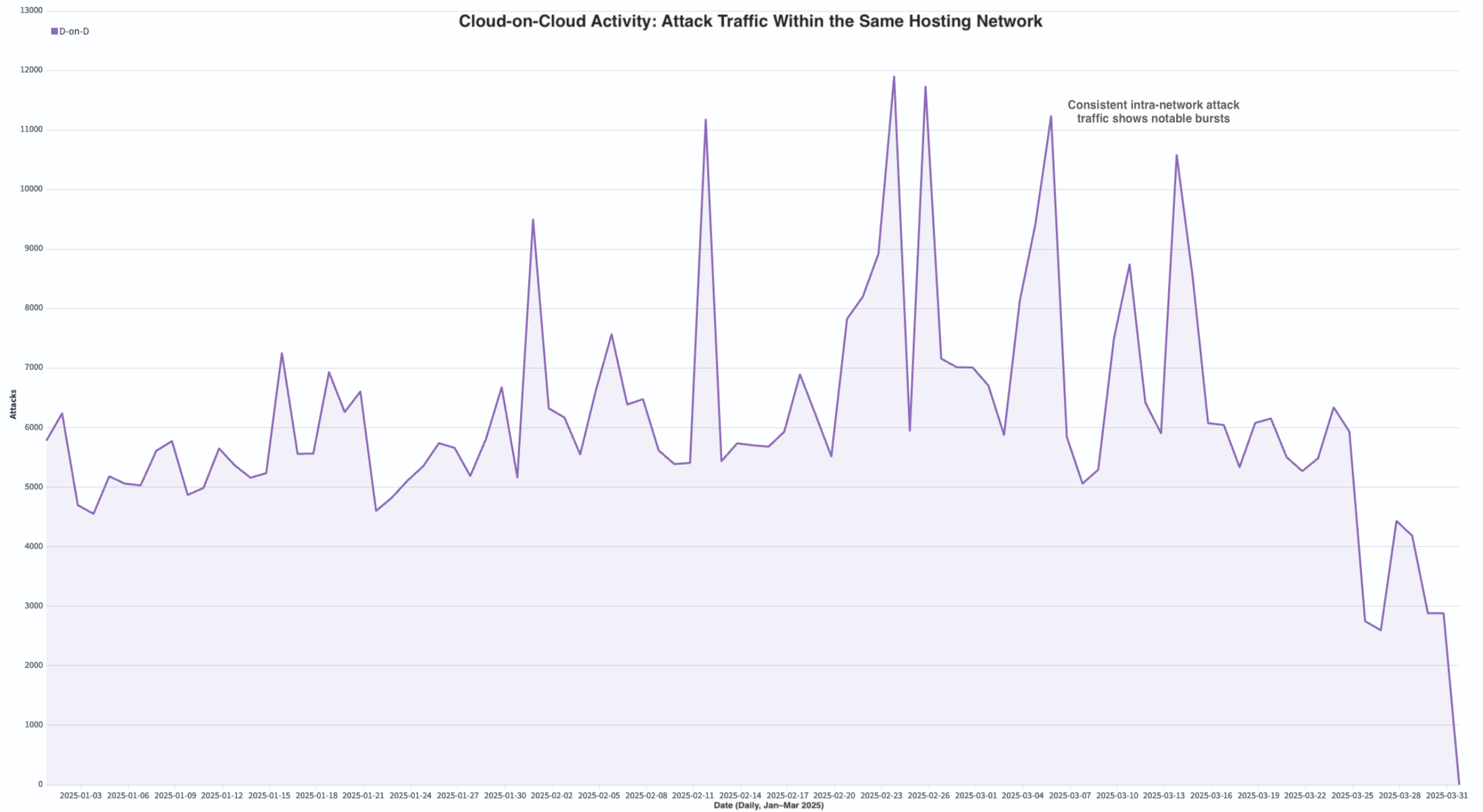
INCLUDING ORGANIZATIONS IN THIS ROOM – Normalized H1 2025



INCLUDING ORGANIZATIONS IN THIS ROOM – Normalized H1 2025, one of these is not like the others...

- "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.




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

GCA'S INTERNET INTEGRITY PROGRAM



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***



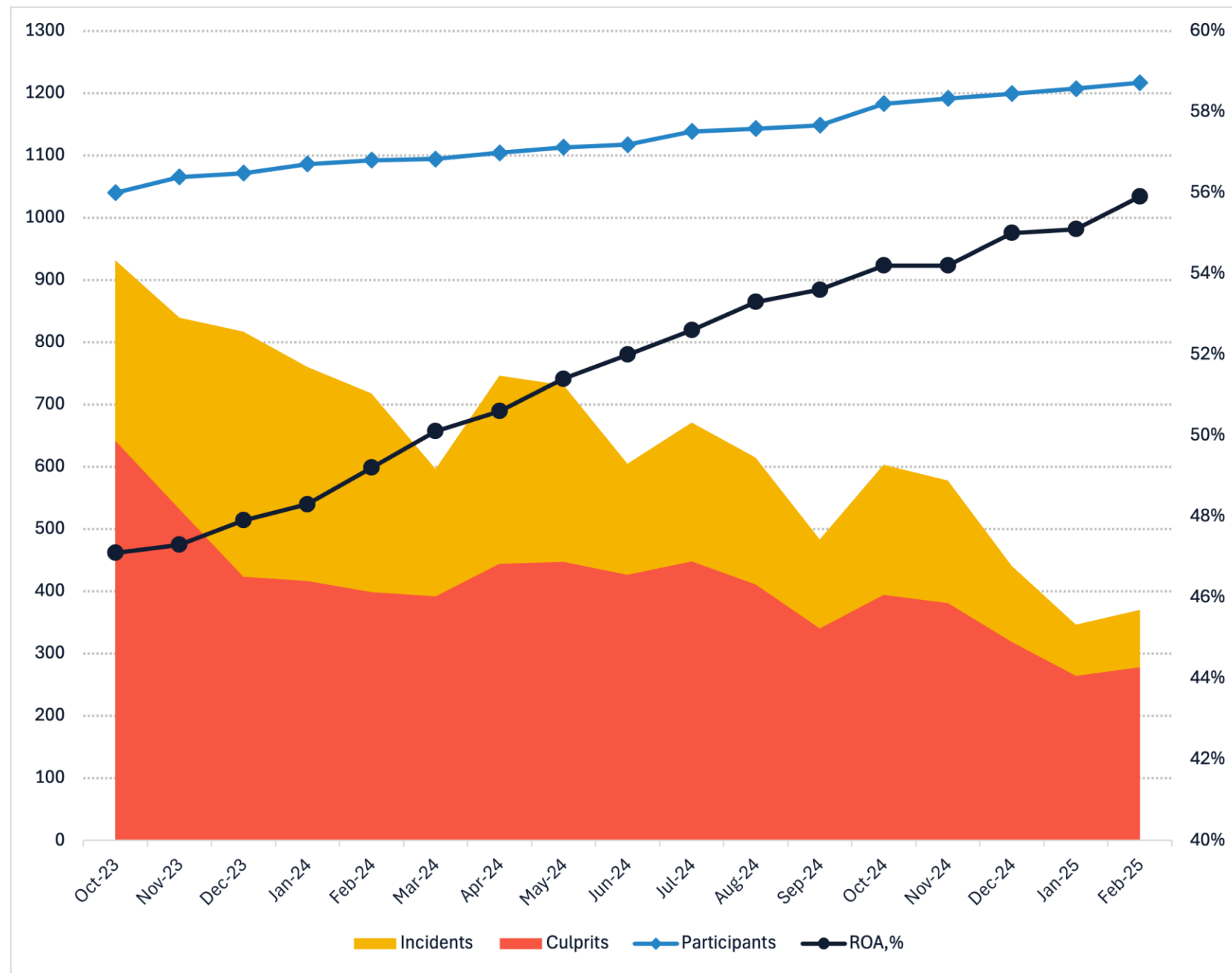
MANRS

THE I2 PROGRAM

ANATOMY OF THE MANRS SUCCESS: THE PRINCIPLES

THE I2 PROGRAM

ANATOMY OF THE MANRS SUCCESS: THE IMPACT?



That was a lot!

You have these slides to refer to

There are references and resources listed at the end of the deck

From all of that, a few things I'd like you to take away...

CONCLUSIONS AND TAKEAWAYS

There are real threats out there in the Internet:

- *They have real impact in the physical world*
- *They are organized and targeted campaigns*
- *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

CONCLUSIONS AND TAKEAWAYS

THANK YOU!

ldaigle@globalcyberalliance.org



Resources

- Attack impacts
 - <https://www.wsj.com/livecoverage/stock-market-today-bank-earnings-07-16-2024/card/unitedhealth-profit-weighed-down-by-cyberattack-disruptions-OagIPtE8A9piNunhWaK8>
 - <https://nypost.com/2023/07/08/large-global-law-firms-affected-by-massive-data-brach/>
 - <https://www.csoonline.com/article/644219/the-real-impact-of-cybersecurity-breaches-on-customer-trust.html>
 - <https://www.bleepingcomputer.com/news/security/cloudflare-blames-recent-outage-on-bgp-hijacking-incident/>
- APT36
 - <https://www.cyfirma.com/research/apt36-phishing-campaign-targets-indian-defense-using-credential-stealing-malware/>
- RedTail
 - <https://www.akamai.com/blog/security-research/2024-redtail-cryptominer-pan-os-cve-exploit#:~:text=The%20malware%20file%20name%20%E2%80%9C.,what%20we%20were%20dealing%20with.>
- Kimsuky
 - <https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/>
 - <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a>
- Dark Pink
 - <https://www.infosecurity-magazine.com/news/dark-pink-apt-group-expands/>
 - <https://socradar.io/apt-profile-dark-pink-apt-group/>
- GCA reports
 - <https://globalcyberalliance.org/aide-data-apt36/>
 - <https://globalcyberalliance.org/aide-data-redtail/>
 - <https://globalcyberalliance.org/aide-data-kimsuky/>
 - <https://globalcyberalliance.org/aide-data-darkpink/>