

NETSCOUT®

The DDoS Threat Landscape Report

NANOG 86

Issue 9: 2022-H1

John Kristoff, *Principal Analyst*

john.kristoff@netscout.com

At a Glance...

ATTACK COUNT

6,019,888

A decrease of 2% from
2021-2H

MAX BANDWIDTH

957.9 Gbps

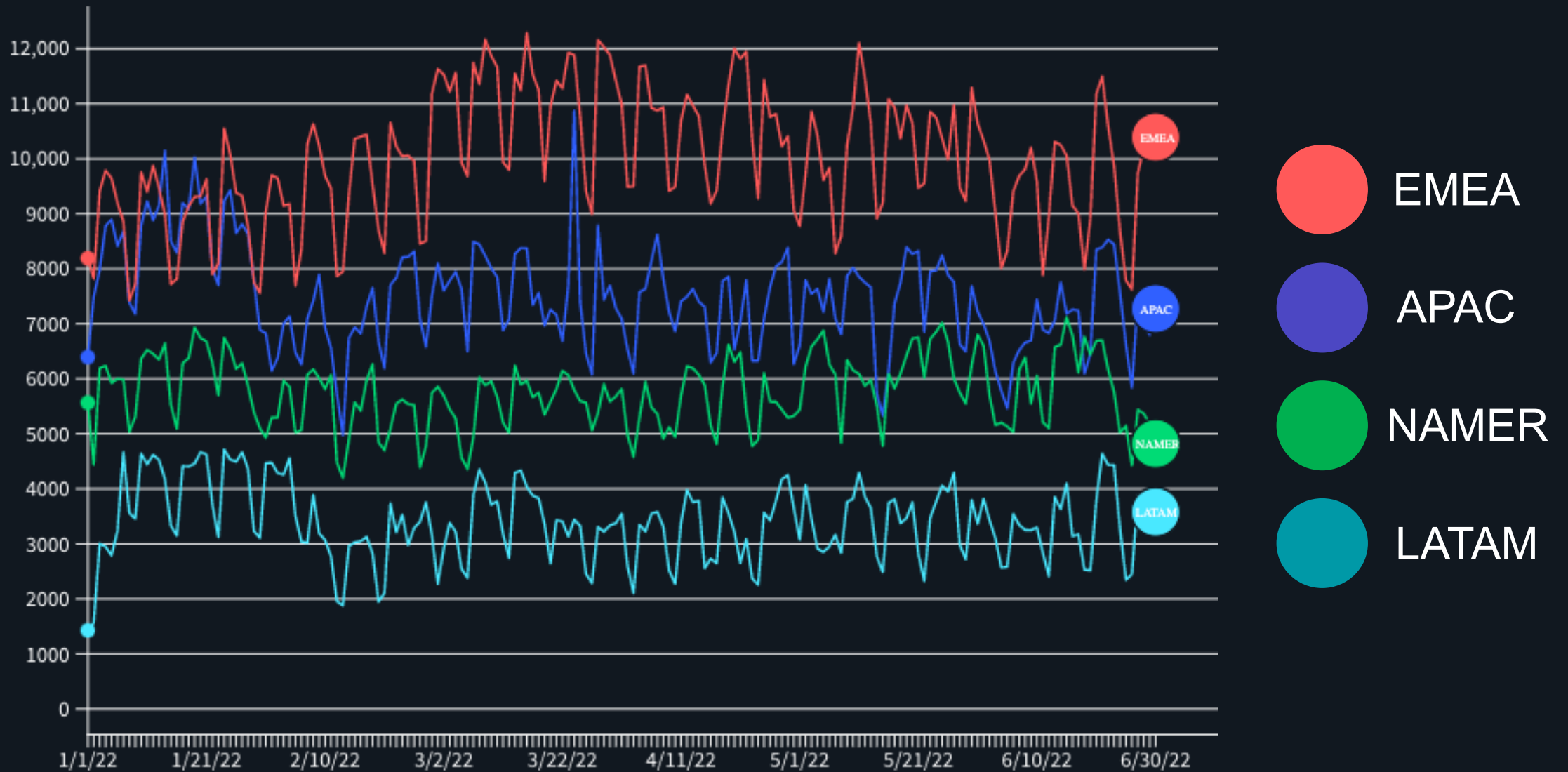
MAX THROUGHPUT

284.4 Mpps

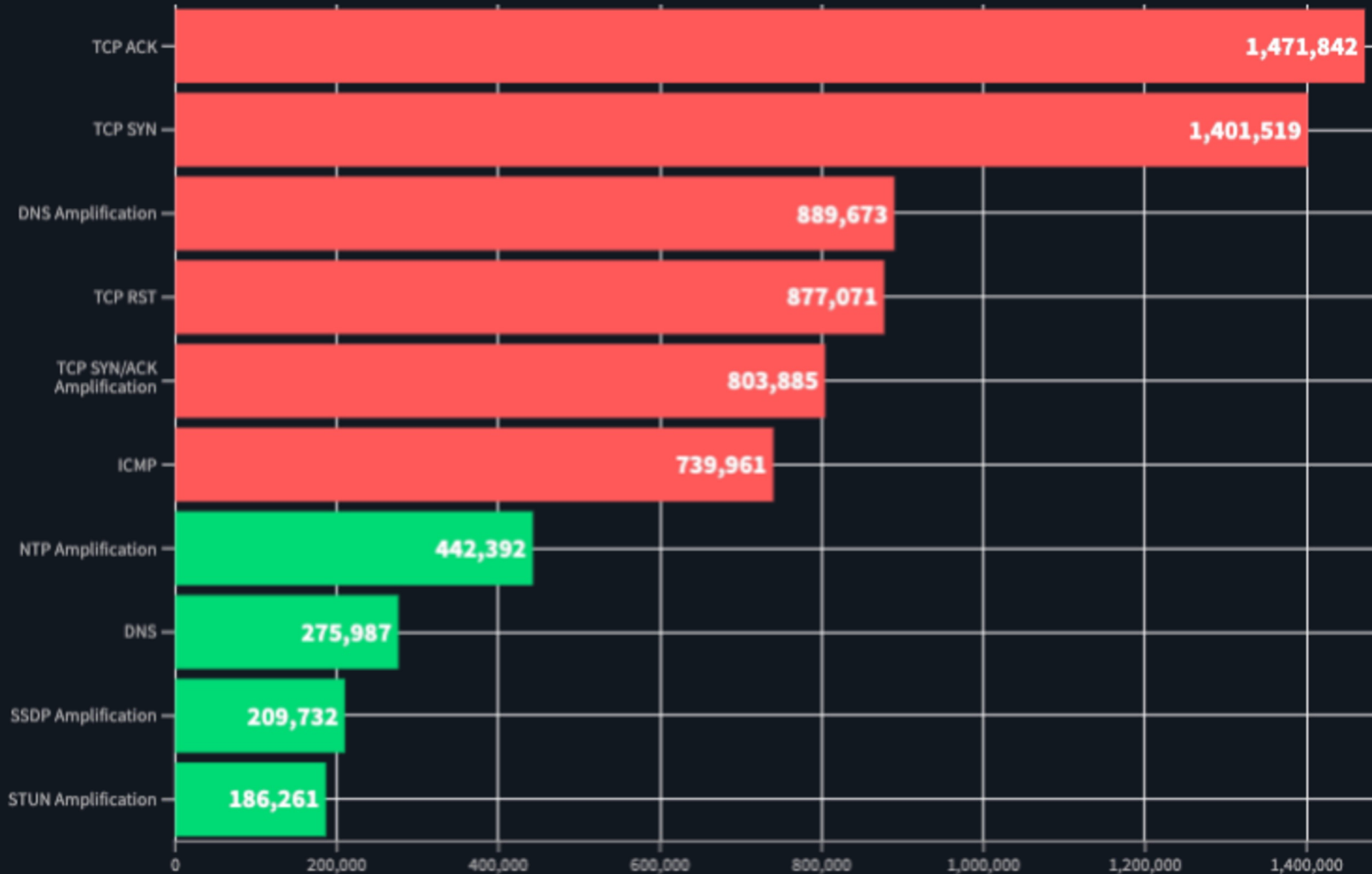
TOP VECTORS

1. TCP ACK
2. TCP SYN
3. DNS Amp
4. TCP RST
5. TCP SYN/ACK Amp

Daily Attack Frequency



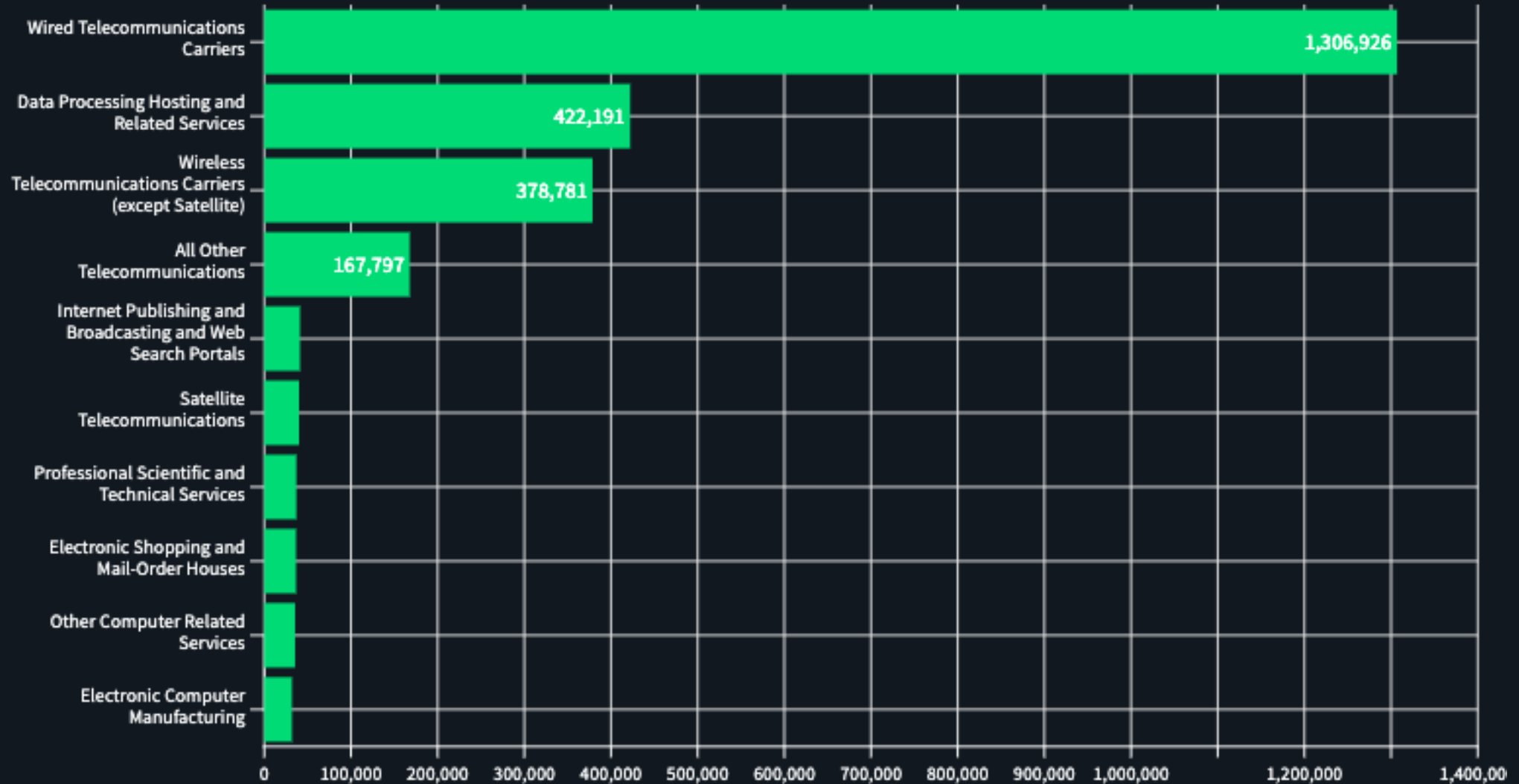
DDoS Global Attack Trends – 2022-H1



VECTOR CHANGES FROM 2021-H2

- TCP ACK **+11%**
- TCP SYN **+20%**
- DNS AMP **-31%**
- TCP RST **+10%**
- TCP SYN/ACK AMP **+21%**

Top Industries Targeted – 2022-H1



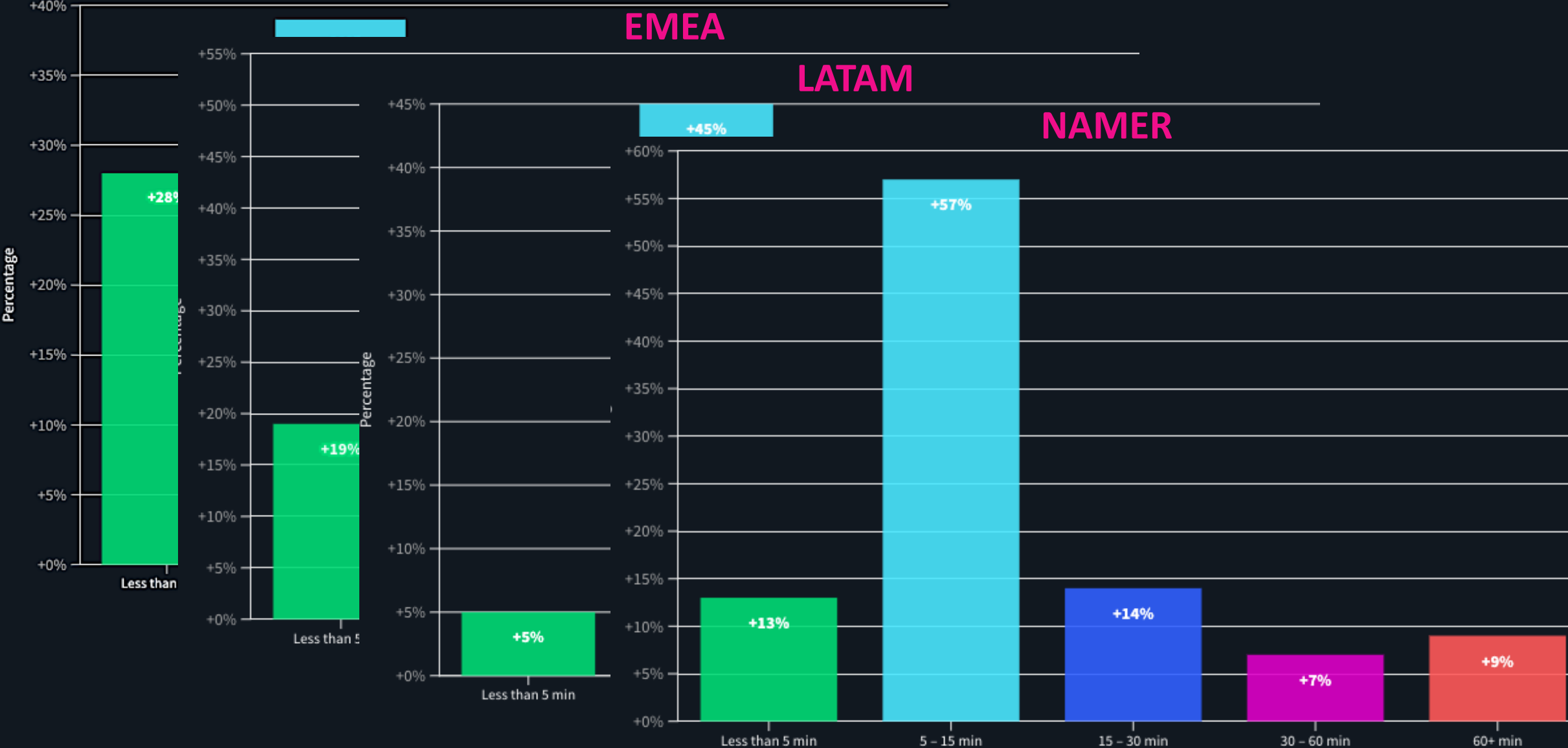
Attack Duration

APAC

EMEA

LATAM

NAMER



The APAC Perspective



NETSCOUT
VISIBILITY

APAC Data was drawn from...

35+

Countries

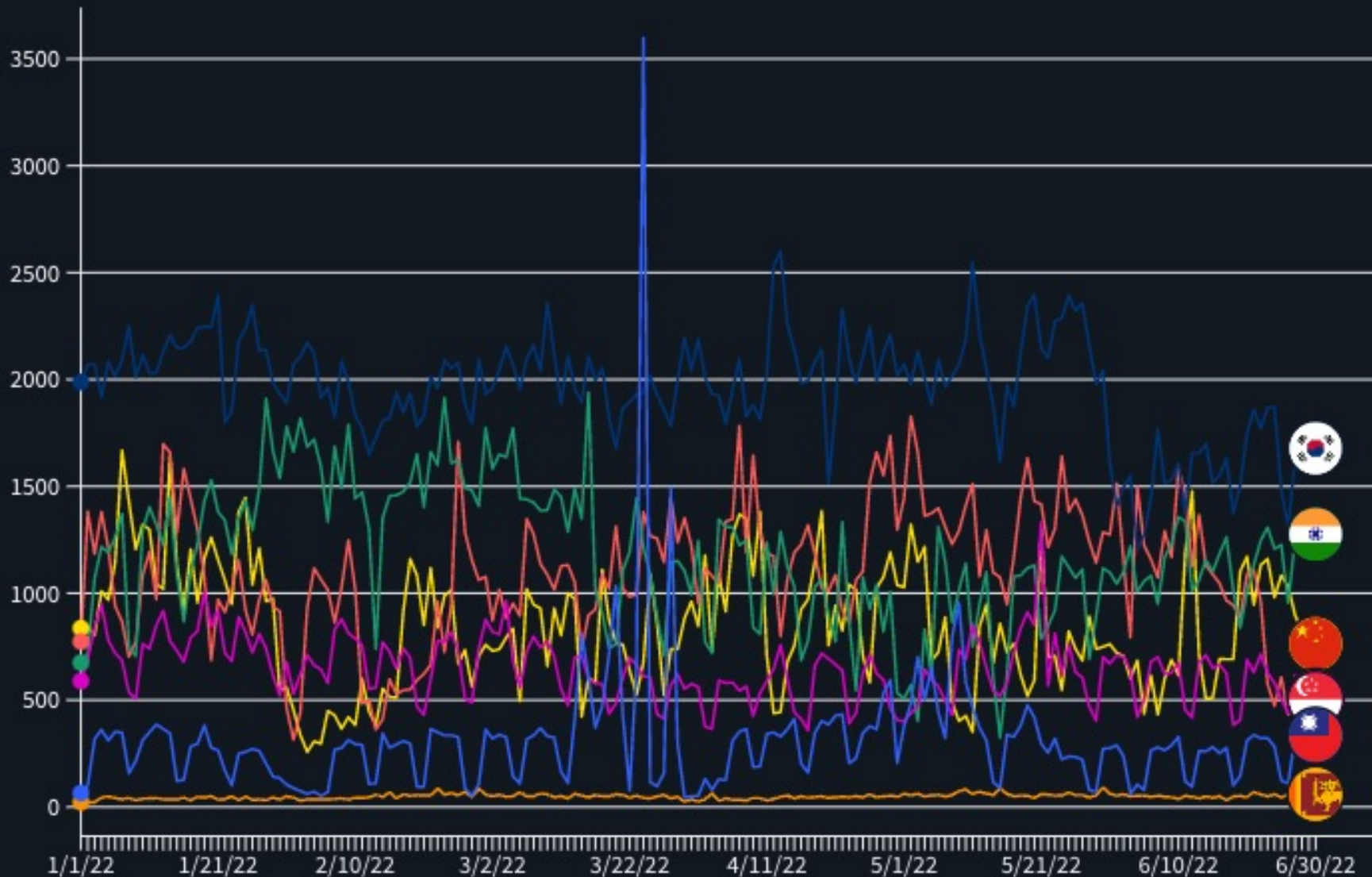
55+

Industry Verticals

4,500+

Autonomous System Numbers (ASNs)

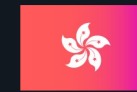
Daily Attacks by Country - APAC



South Korea accounted for 26% of all attacks in APAC



Taiwan experienced nearly 3,600 attacks coinciding with public remarks in support of Ukraine



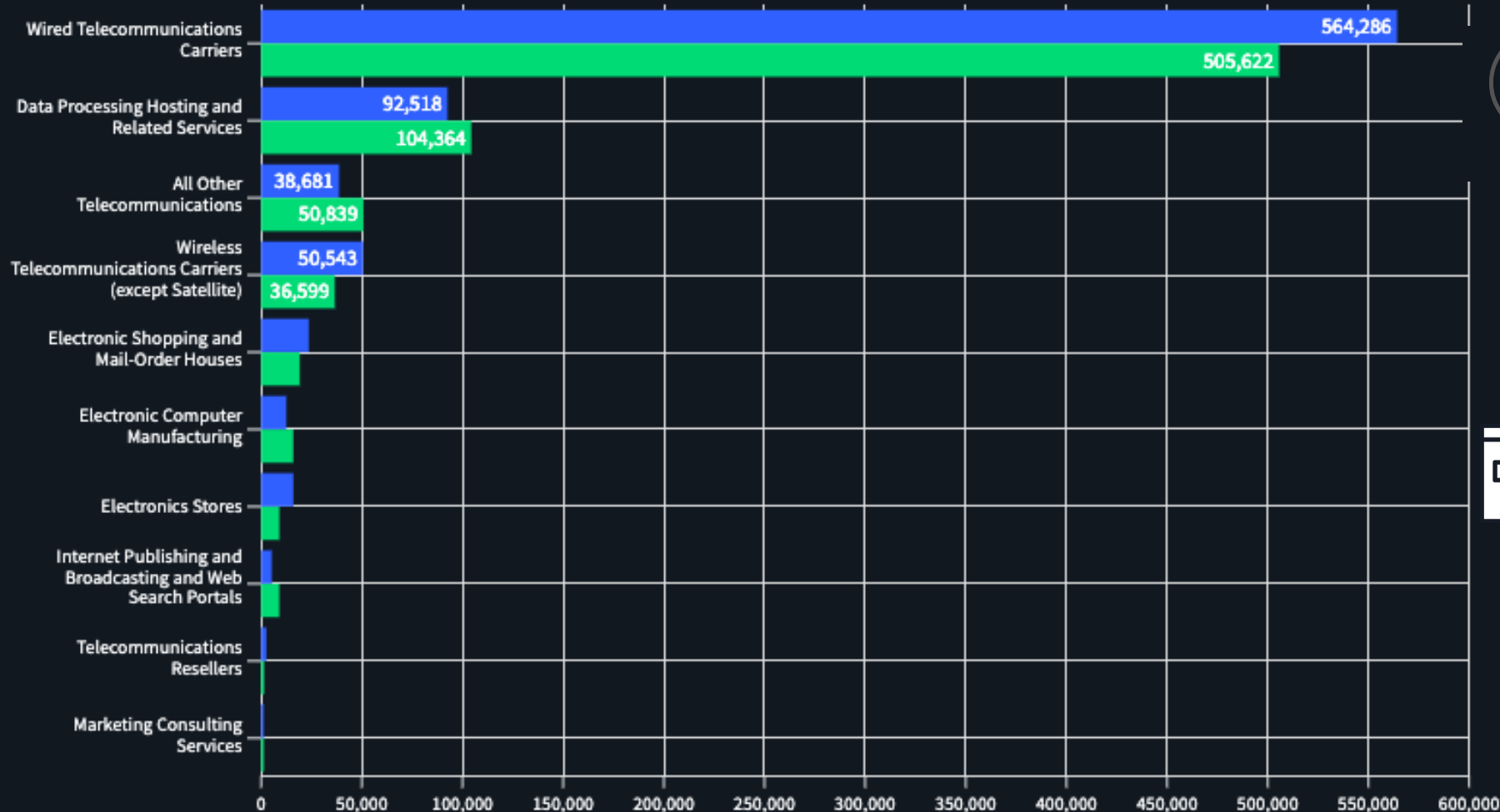
Attacks in Hong Kong and China follow also



coincided with fluctuations in regional and global tensions.

Top Industries Targeted - APAC

● 2H 2021 ● 1H 2022



All Other Telecommunications (think VoIP) experienced a 59% increase in 2021 and another 31% increase in 2022



Internet Publishing & Broadcasting (Zoom, Netflix, etc.) experienced a 72% increase, a move contrary to the global trend of a decrease.

The EMEA Perspective



NETSCOUT
VISIBILITY

APAC Data was drawn from...

128

Countries &
Territories

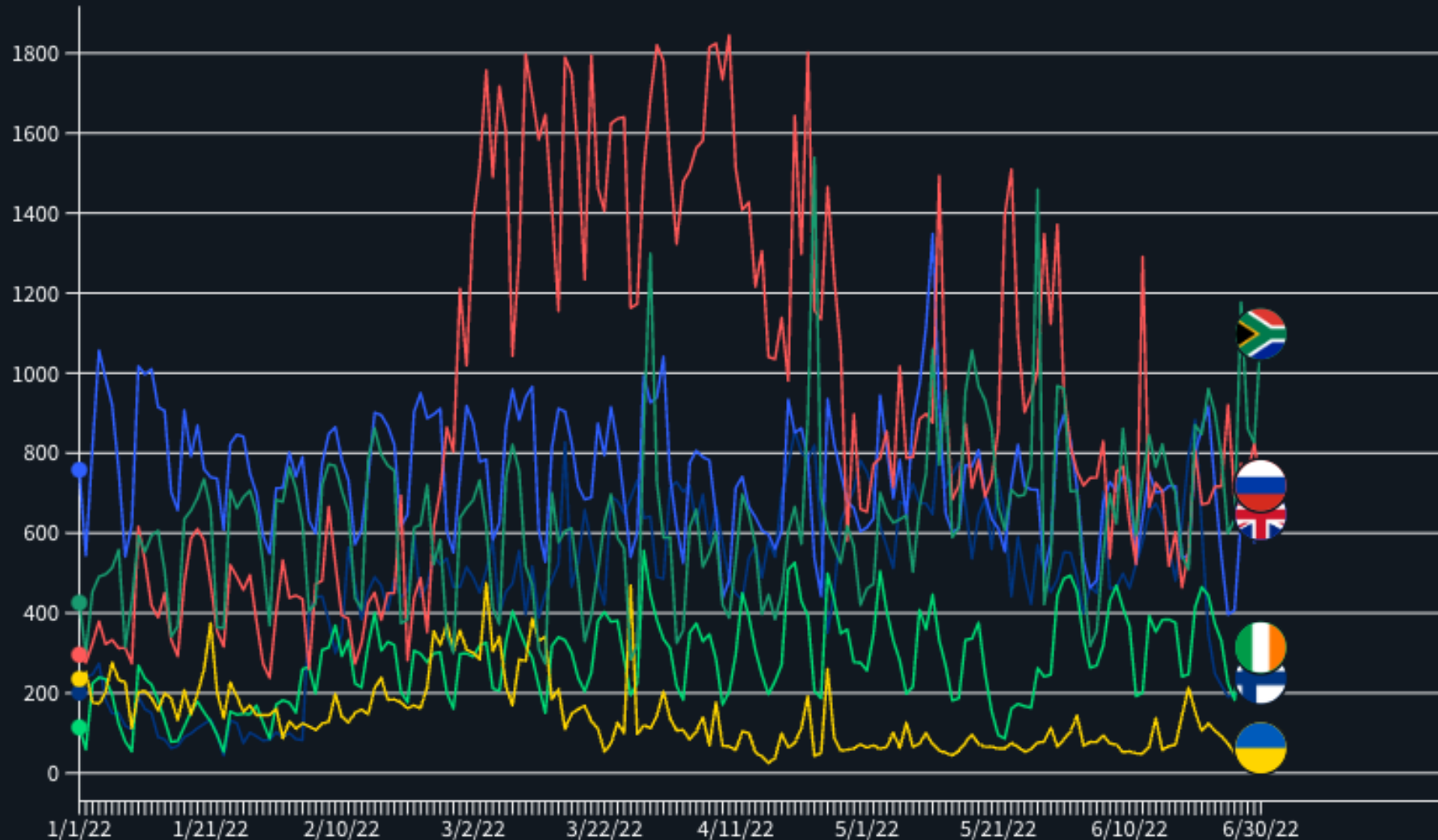
150+

Industry Verticals

13,500+

Autonomous System Numbers (ASNs)

Daily Attacks by Country - EMEA



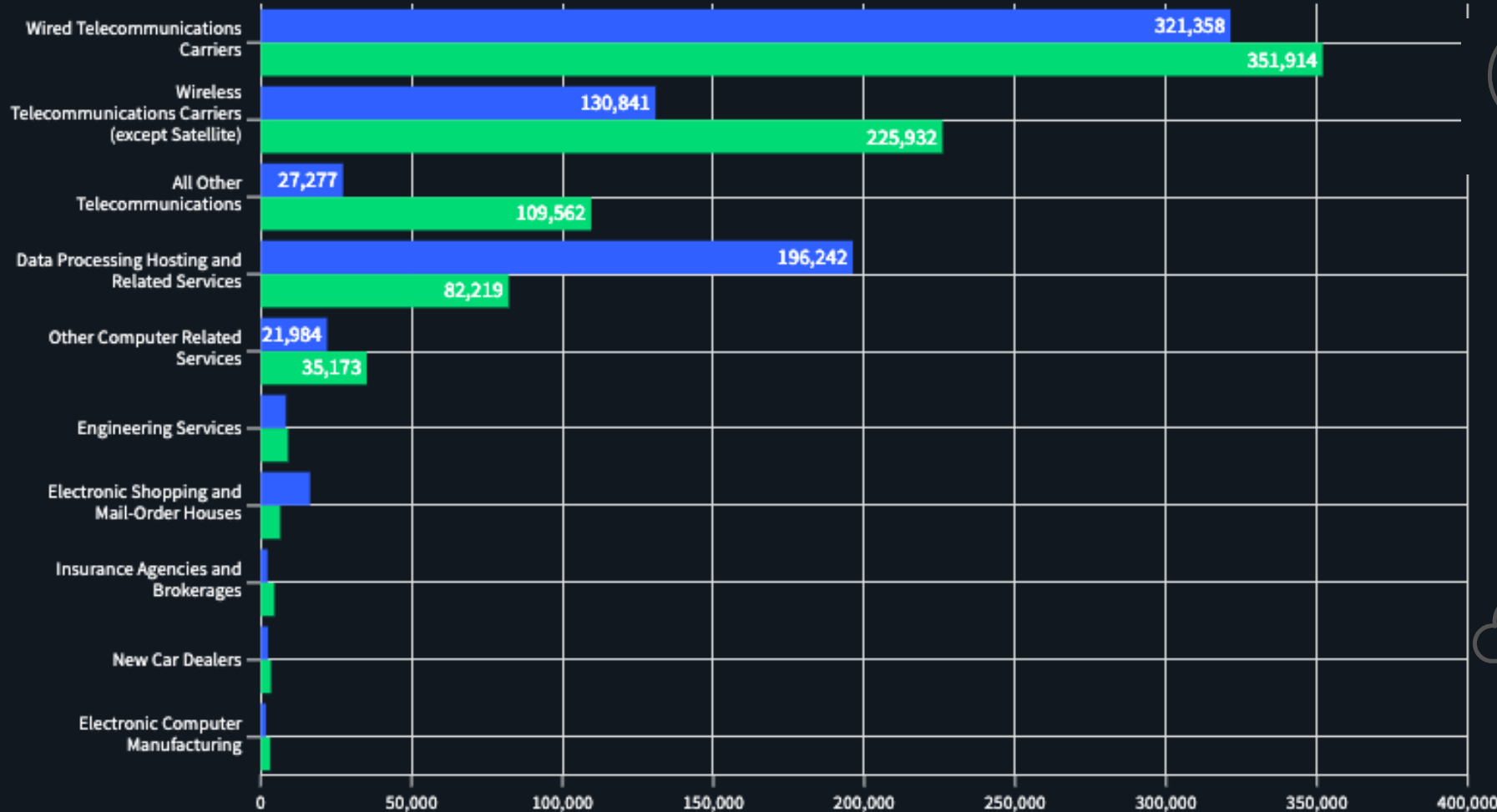
Attacks in South Africa started to rise in May and ended the period as the highest daily total of the top attacked countries in EMEA.



Russia experienced a 3x sustained increase in attacks since the start of the year.

Top Industries Targeted - APAC

● 2H 2021 ● 1H 2021



All Other Telecommunications (think VoIP) experienced a 302% increase.



Wireless Telecommunications experienced a 73% increase;



While Data Processing, Hosting, and Related Services (cloud) experienced a 58% decrease.

The LATAM Perspective



NETSCOUT
VISIBILITY

LATAM Data was drawn from...

40+

**Countries &
Territories**

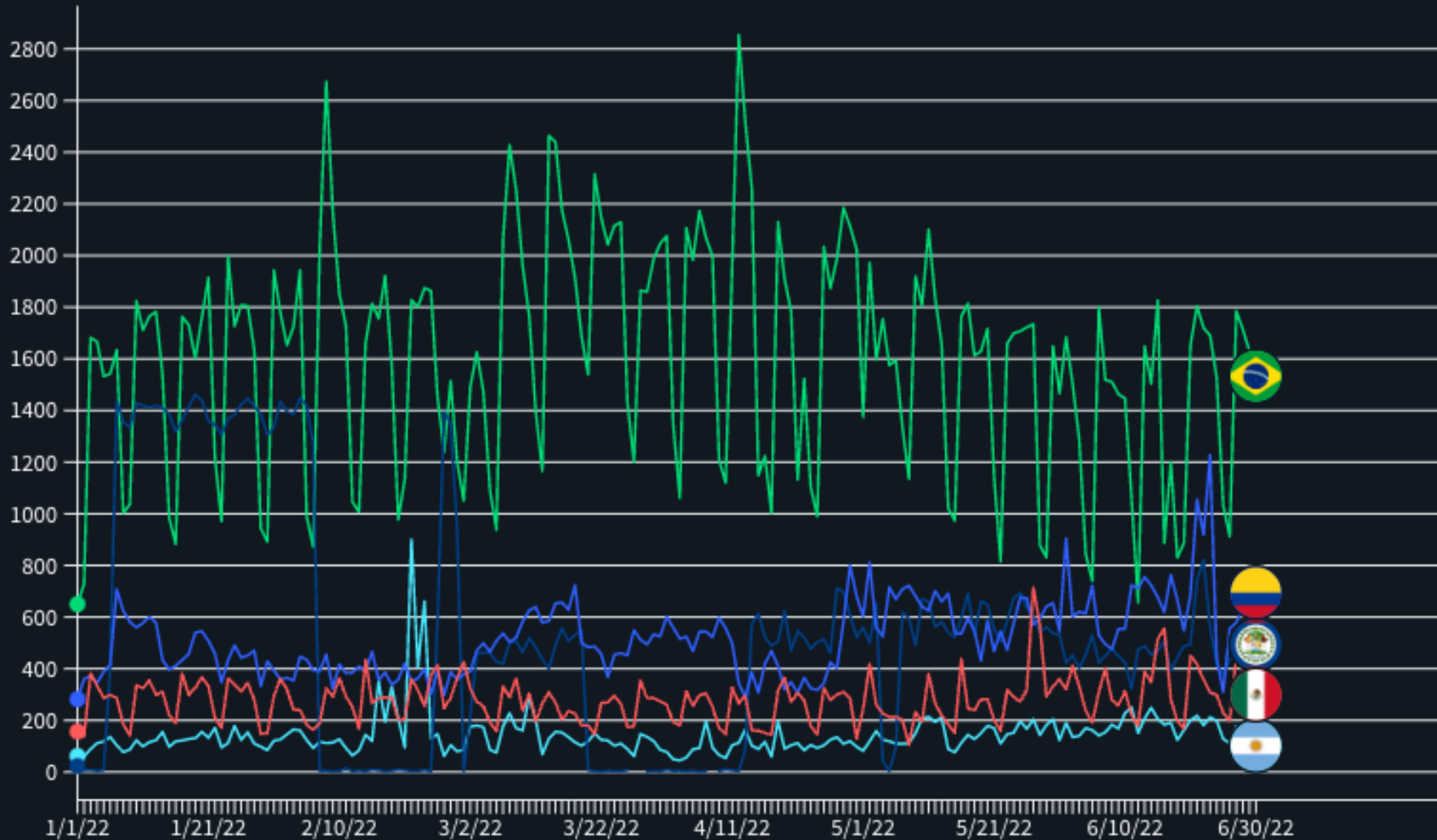
60

Industry Verticals

9,000+

Autonomous System Numbers (ASNs)

Daily Attacks by Country - LATAM



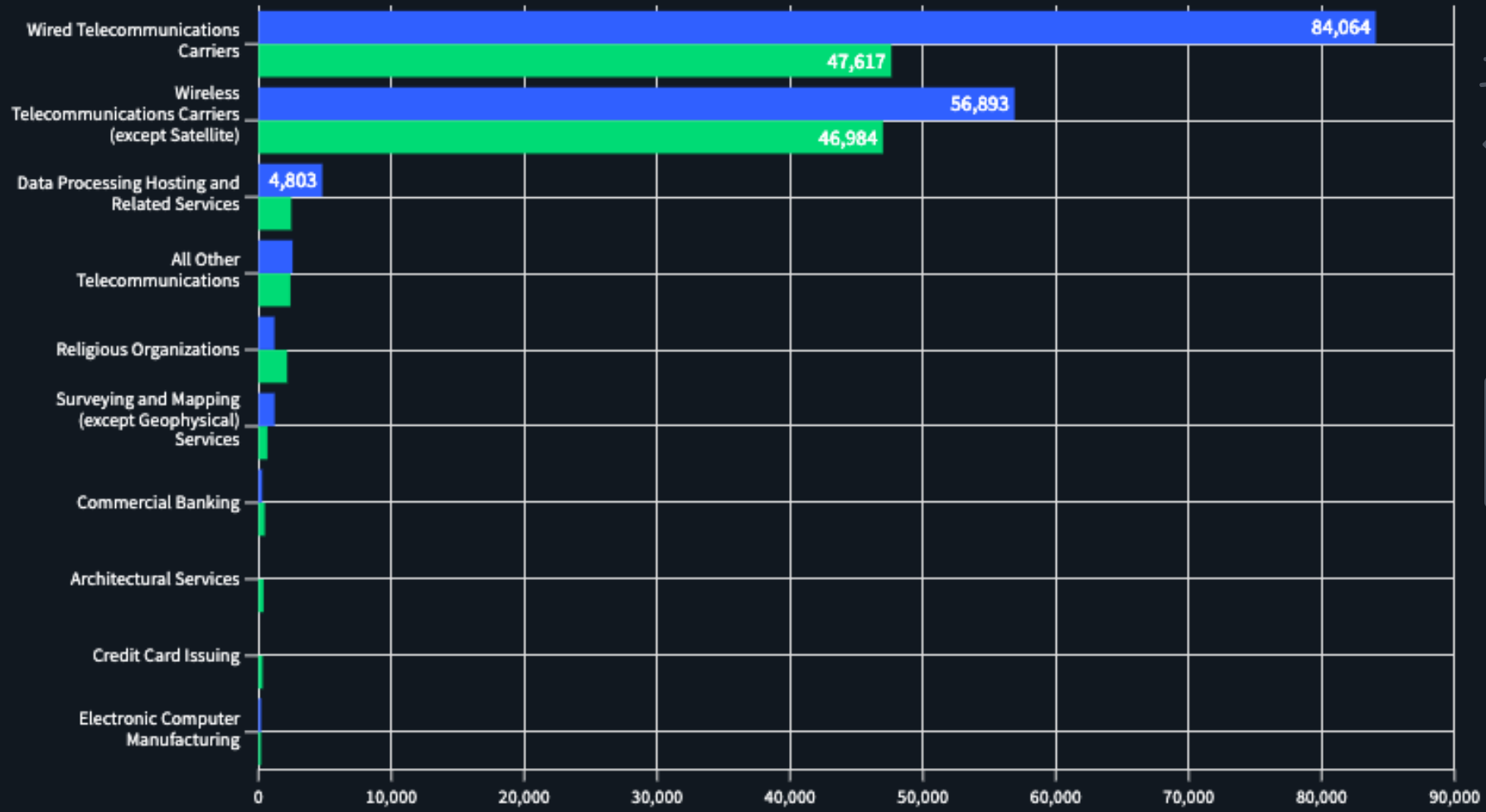
Brazil accounts for more than 50% of all daily attacks in LATAM.



Attacks surges in Columbia coincided with their presidential election and the subsequent runoff election.

Top Industries Targeted - LATAM

● 2H 2021 ● 1H 2022



Religious organizations in Brazil saw a significant increase in TCP-based attacks sourced from botnets.



Commercial banking experienced a 63% increase in attacks while credit card issuers came into focus with hundreds of attacks for the first time.

The NAMER Perspective



NETSCOUT.
VISIBILITY

NAMER Data was drawn from...

4

Countries

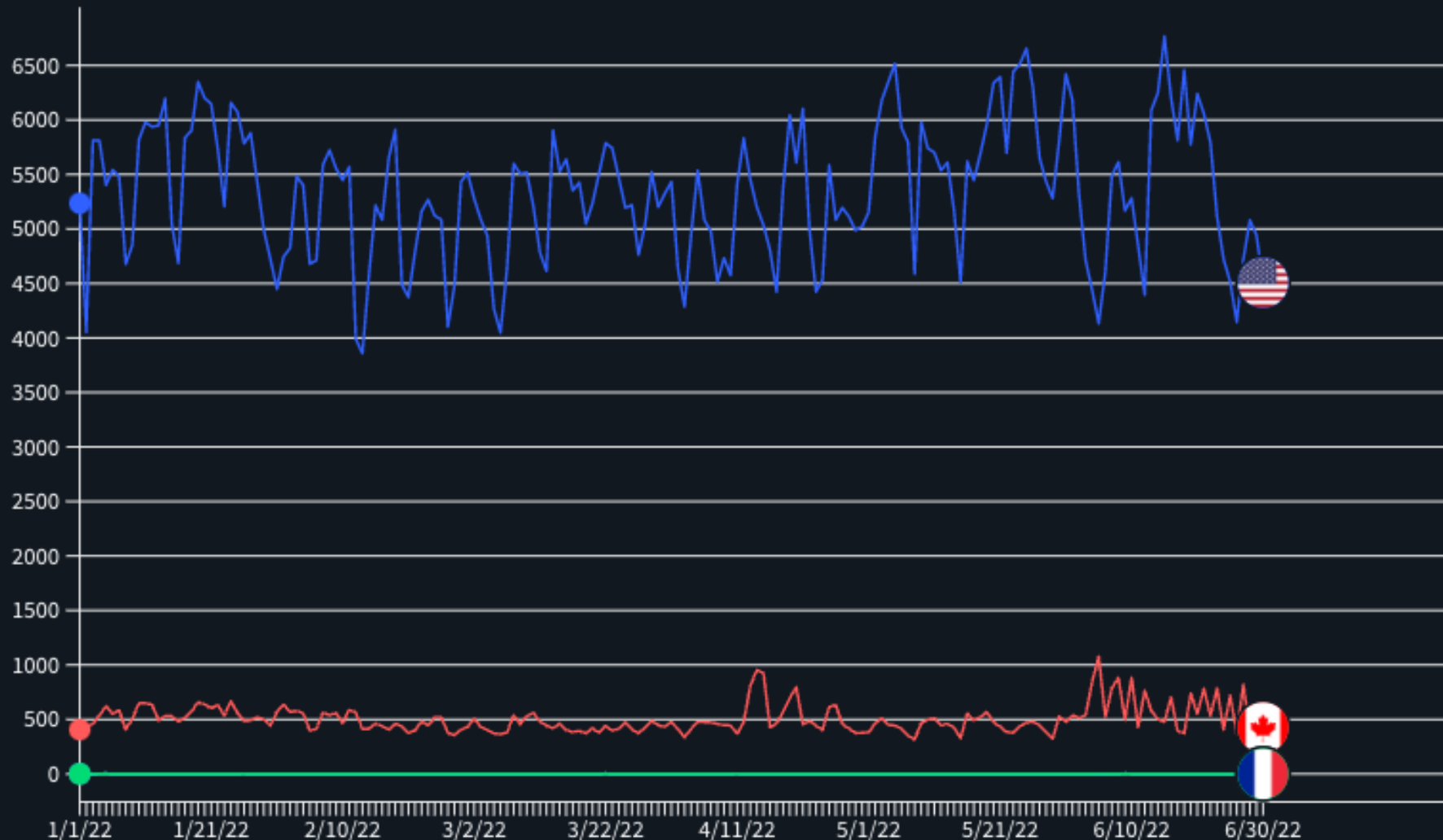
150+

Industry Verticals

5,785

Autonomous System Numbers (ASNs)

Daily Attacks by Country - NAMER



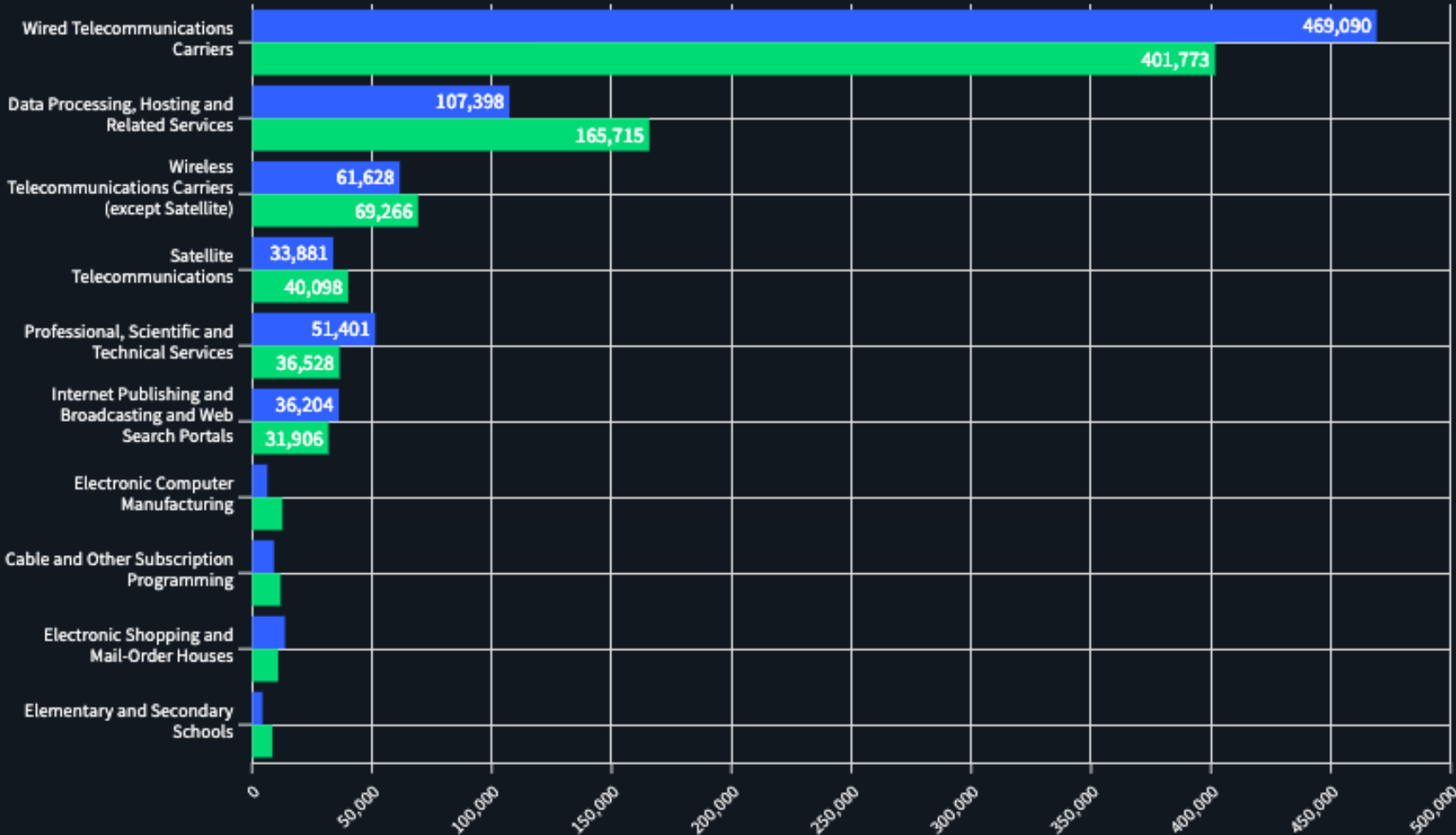
While Canada does account for some of the attacks against NAMER, the vast majority are against entities in the United States of America.



- The increase in attacks beginning in March coincides with an uptick in attacks on satellite telecommunications and cloud hosting providers in the USA.

Top Industries Targeted - NAMER

● 2H 2021 ● 1H 2021



Cloud hosting providers experienced a 54% increase in attacks.

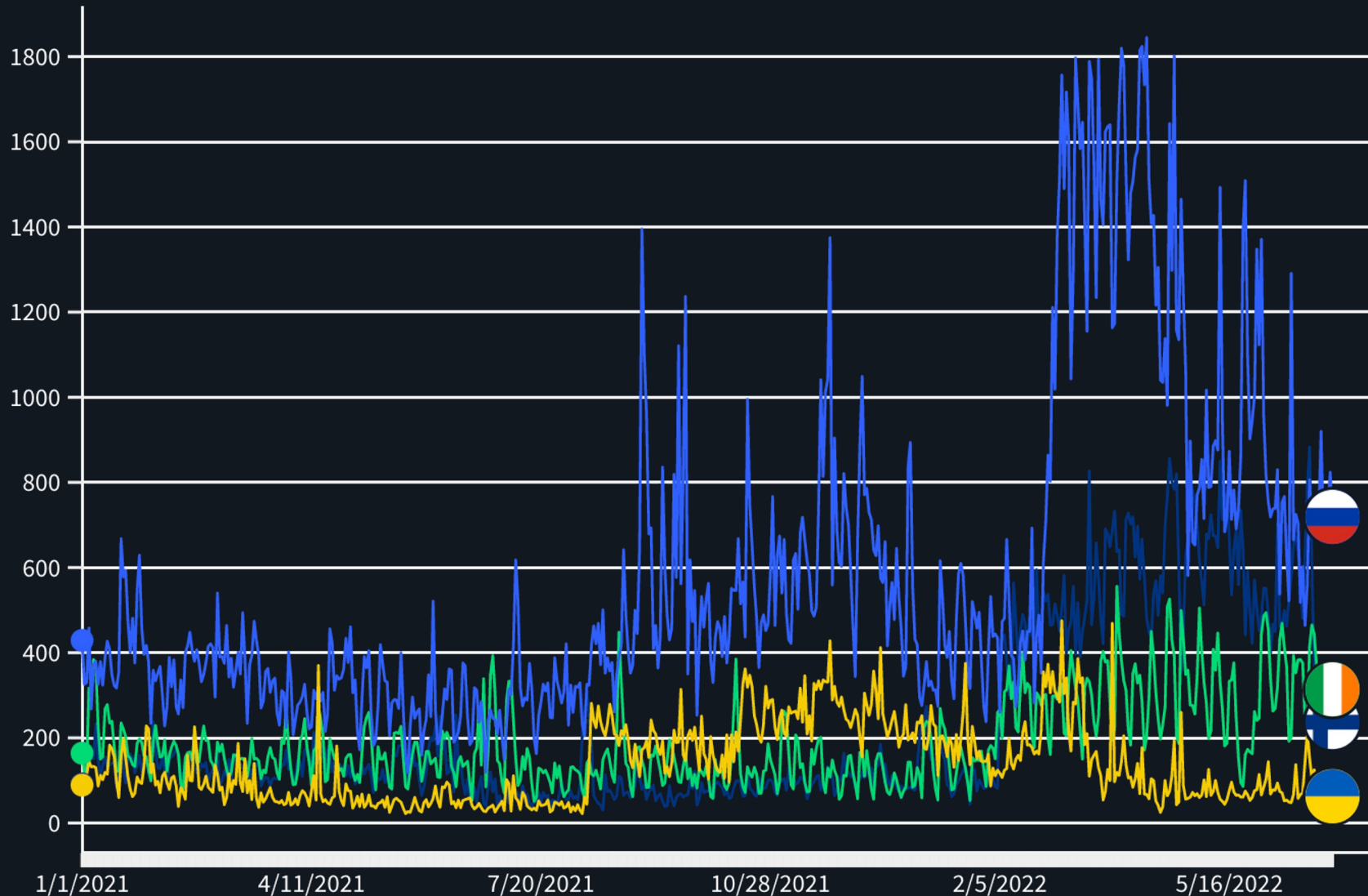


Satellite Telecommunications witnessed an 18% increase in attacks.



Elementary Education was hit hard in the first half of the year with a 95% increase in attacks, largely sourced from free attack tools and services.

Russia, Ukraine, and the Ripple Effect



Ukraine experienced a surge in attacks between late February and mid March



Shortly after their invasion into Ukraine, Russia experienced a tripling of daily attacks that carried well into June.

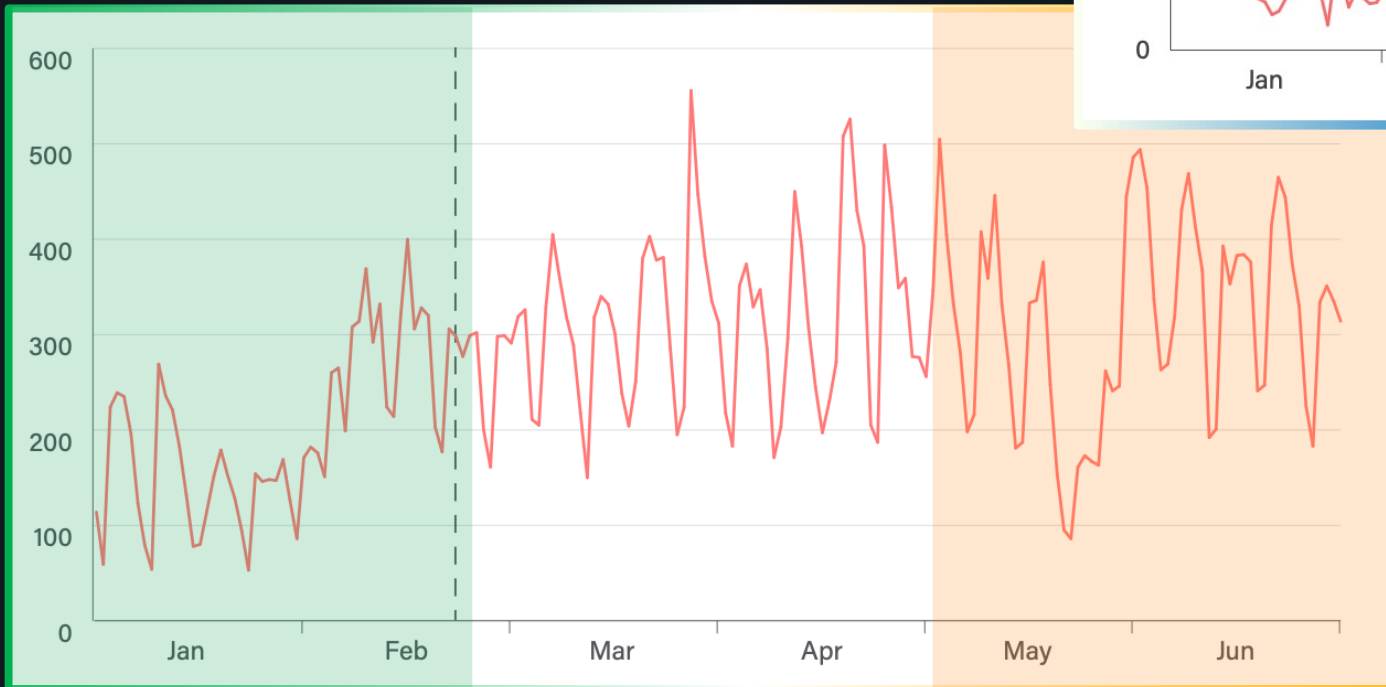
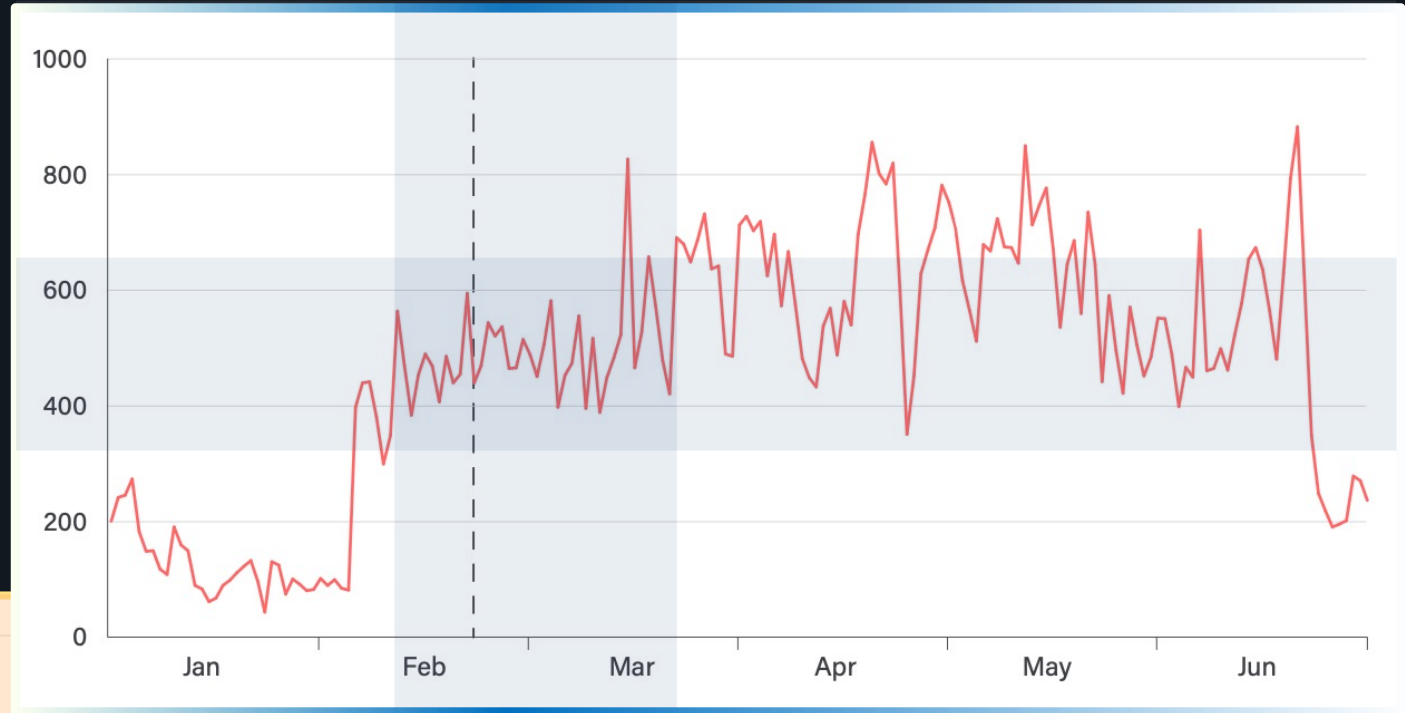


Finland re-engaged in talks to join NATO in early February and since then have more than doubled daily DDoS Attacks

The Ripple Effect

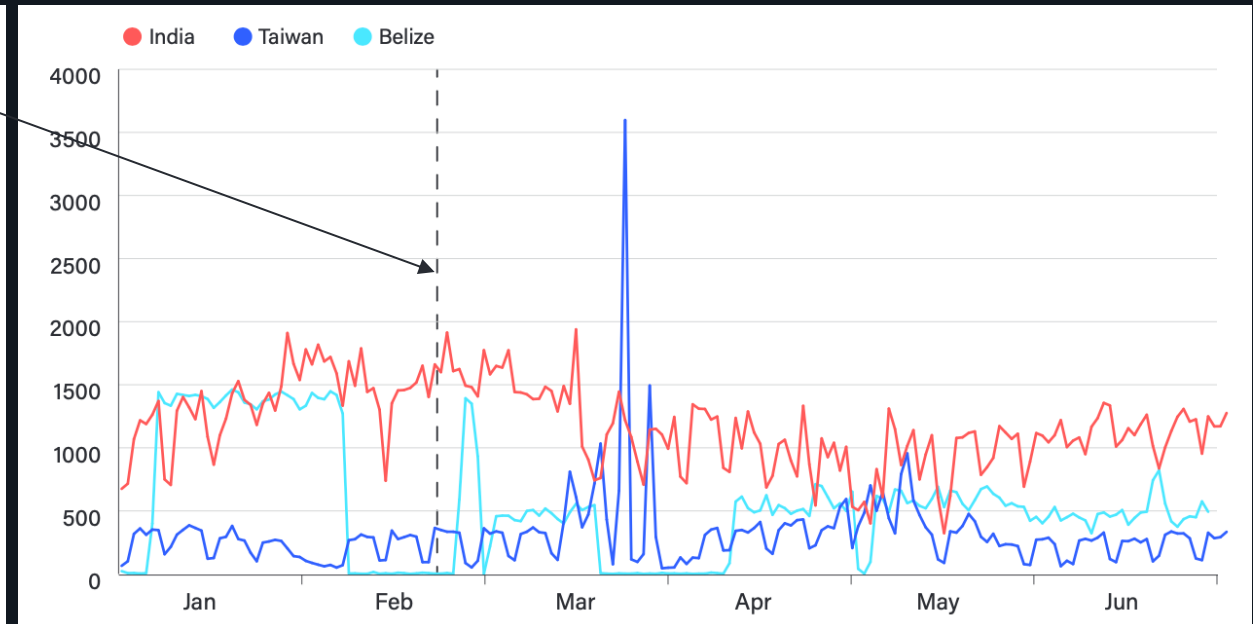
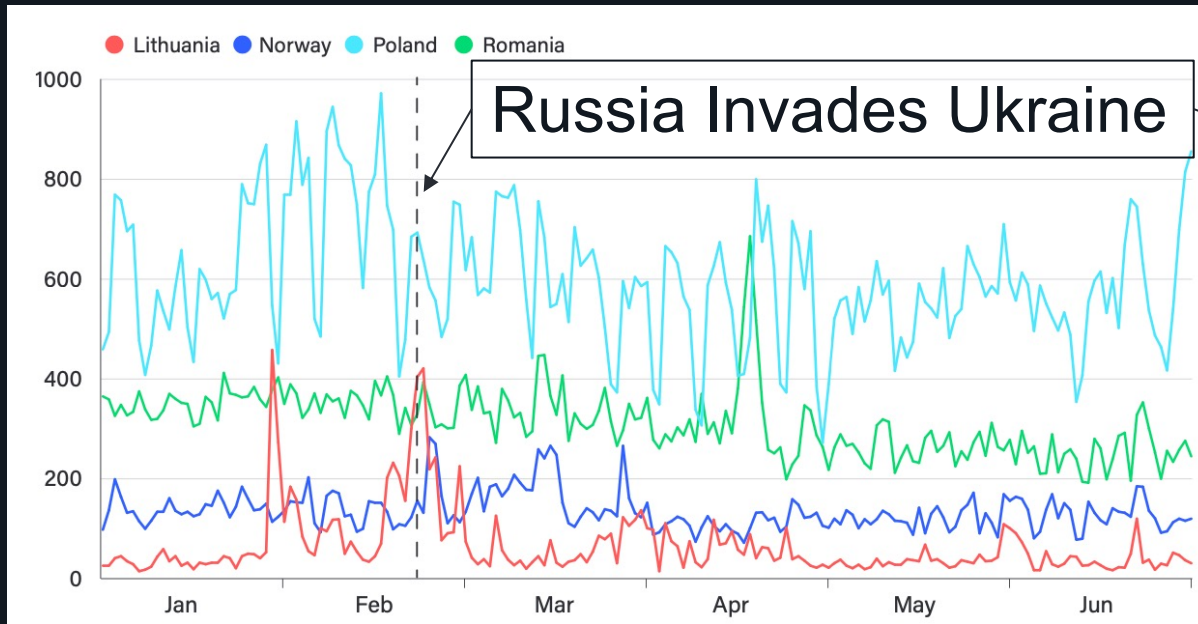


Finland re-engaged in discussions to join NATO with rumors of Russia's invasion into Ukraine and confirmed commitment following ground operations.



Ireland experienced a sustained and significant increase in attacks as Ukrainian infrastructure was offloaded to the country.

Words and Actions Can Cause Ripples

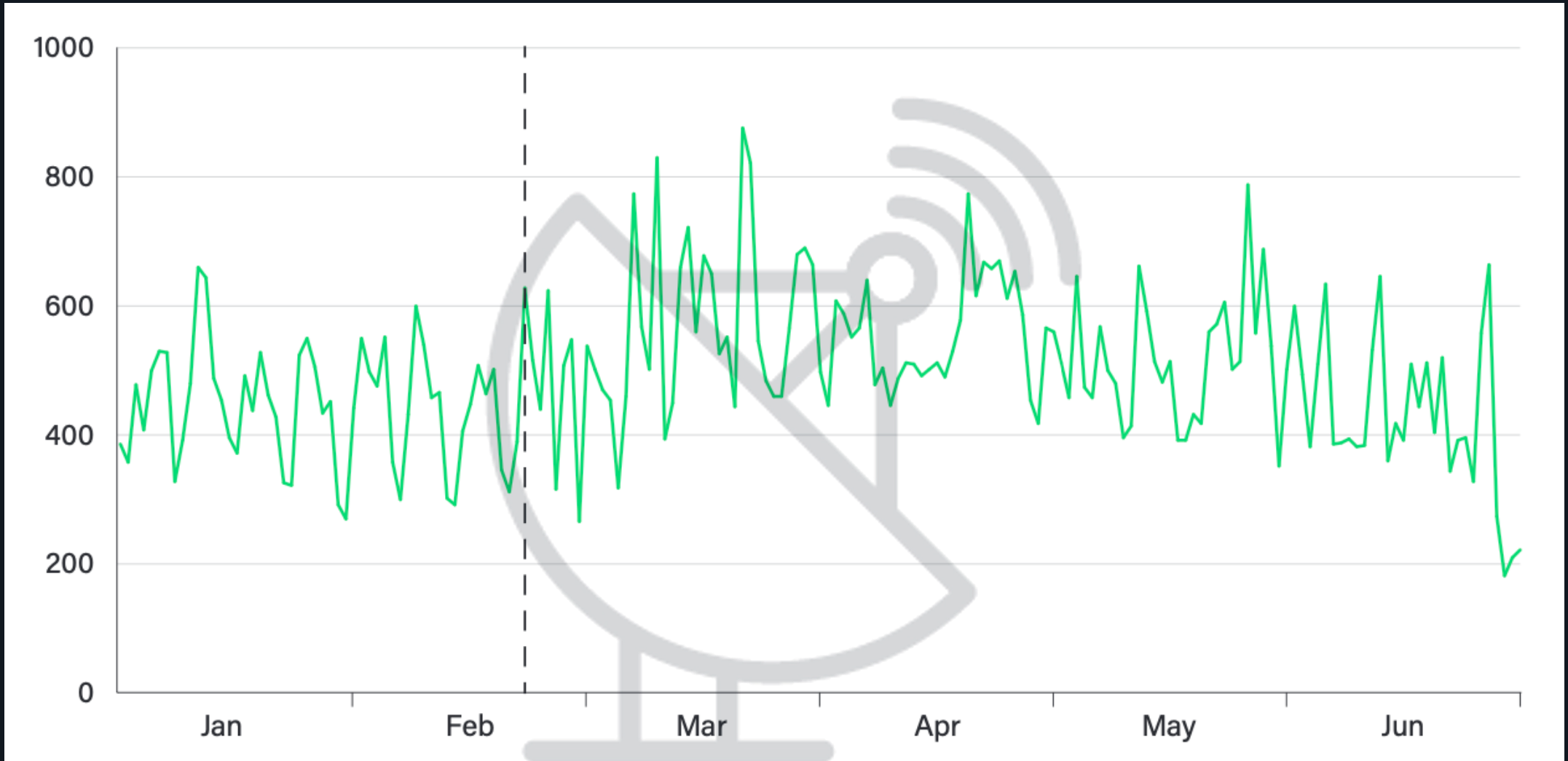


- Killnet Threats – June 27, 2022
- Killnet Threats – June 30, 2022
- Killnet Threats – July 11, 2022
- Killnet Threats – April 29, 2022

- Ukrainian Nationals Protest in Teipei – June 30, 2022
- Belize government remarks publicly on “illegal” invasion of Ukraine

Industry Feels the Ripple


Satellite Telecommunications



Also see: <https://www.netscout.com/threatreport/>

REGIONAL HIGHLIGHTS


Asia Pacific



LEARN MORE →

REGIONAL HIGHLIGHTS


Europe, Middle East, and Africa



LEARN MORE →

REGIONAL HIGHLIGHTS


Latin America



LEARN MORE →

REGIONAL HIGHLIGHTS

North America



LEARN MORE →

01

War, Religion, and Politics: A Battleground For DDoS



LEARN MORE →

02


Adaptive DDoS Attacks and Learning How to Suppress Them



LEARN MORE →

03

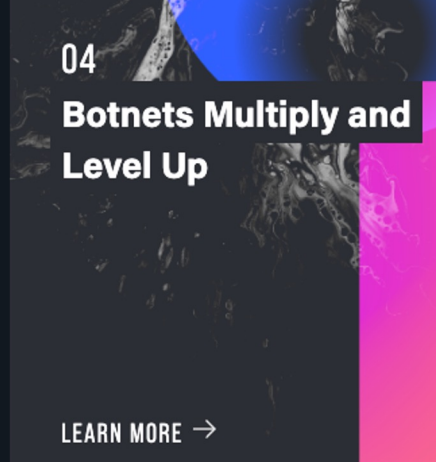
Adversaries Evolve and Innovate Attack Methods and Vectors



LEARN MORE →

04

Botnets Multiply and Level Up



LEARN MORE →

Thank you.

If you have any questions about the material presented,
please feel free to send email to discuss!

john.kristoff@netscout.com

[netscout.com](https://www.netscout.com)