NETSCOUT

A Year Like No Other

DDoS in a Time of Pandemic

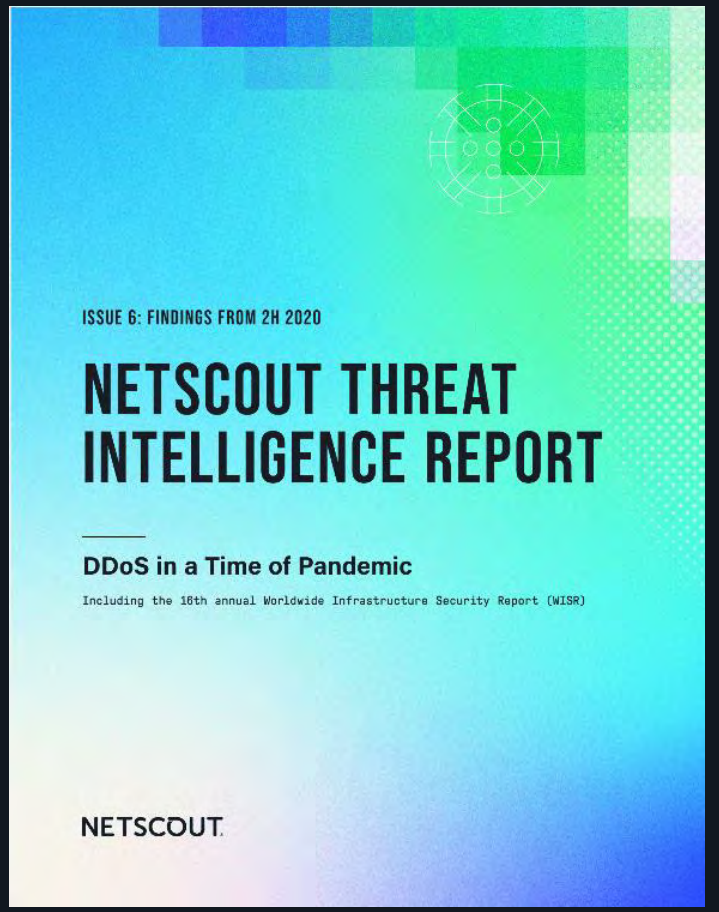
Roland Dobbins <roland.dobbins@netscout.com>

Principal Engineer

6th NETSCOUT Threat Intelligence Report

Including the 16th Annual WISR Results

- Data-driven survey of the DDoS threat landscape
  - Trends and analysis of global internet traffic collection
  - Fuses operational experience and expertise with real-world DDoS attack telemetry
  - Firsthand observations in the IoT threat space and how adversaries abuse devices to launch DDoS attacks
- 16th Annual WISR
  - ISP and enterprise concerns, current security priorities, and future outlook.



https://www.netscout.com/threatreport

Agenda

- Key Findings
- Global Attack Trends
- Lazarus Bear Armada (LBA)
- Regional & County Statistics
- Internet of Things (IoT)

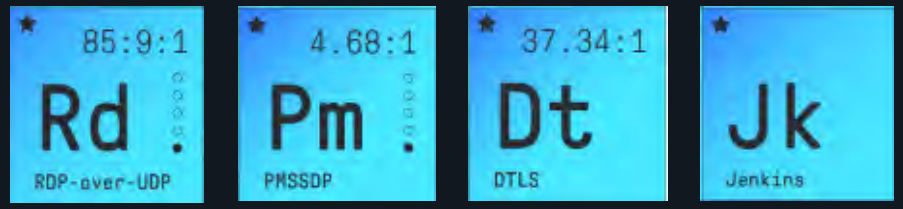
NETSCOUT

Key Findings

Global DDoS Attack Summary

Key Findings

- Record-breaking number of DDoS attacks
  - A 20% Increase year-over-year
- DDoS attacks reached a new cadence
  - 800,000+ Attacks per month; Nearly 130,000 more attacks per month on average
- Adversaries added new DDoS vectors to their toolkit



- Lazarus Bear Armada (LBA) global DDoS extortion campaign
  - 275 different organizations, in 40 distinct industries, across 55 countries

NETSCOUT

Global DDoS Attack Trends

Regional Summaries

Global Statistics

2020 Review

Max attack bandwidth:
1.12 Tbps (EMEA)

Max attack throughput:
581 Mpps (APAC)

Average attack duration:
39.83 Minutes

Max attacks/month:
929,000+ May 2020

NETSCOUT

Lazarus Bear Armada (LBA)

A Global DDoS Extortion Campaign

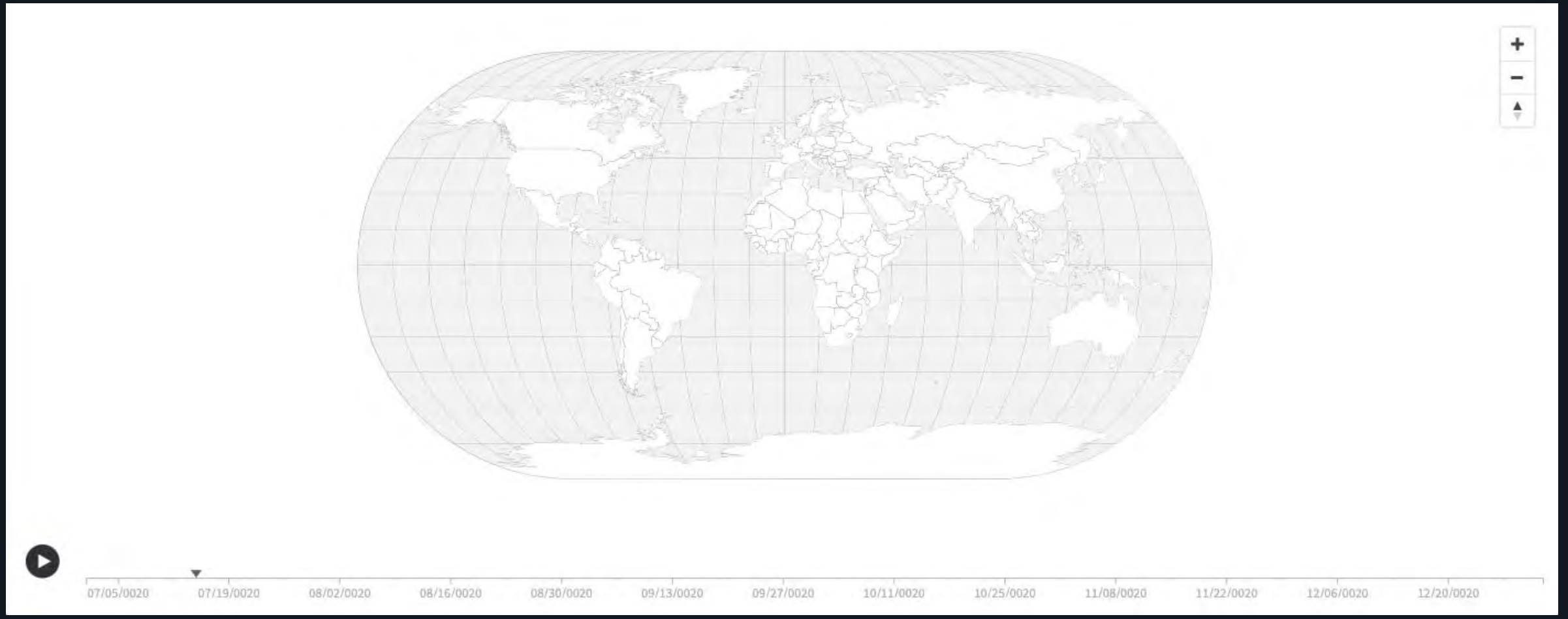
Lazarus Bear Armada (LBA)

Campaign Tracking and Analysis

- Masquerades as Lazarus Group, Fancy Bear, and Armada Collective
  - Labeled **LBA** by NETSCOUT
- Began in early August 2020
  - Targeting financial and financial-adjacent targets.
  - Moved to insurance, broadband access ISPs, transportation & travel, and other verticals when first round of targets refused to pay extortion demands
- Leverages FOURTEEN different DDoS attack vectors and combines with more advanced tactics such as:
  - Targeting VPN concentrators; upstream transit ISPs and DDoS mitigation MSSPs; masquerading attack traffic as VPN traffic; and others.

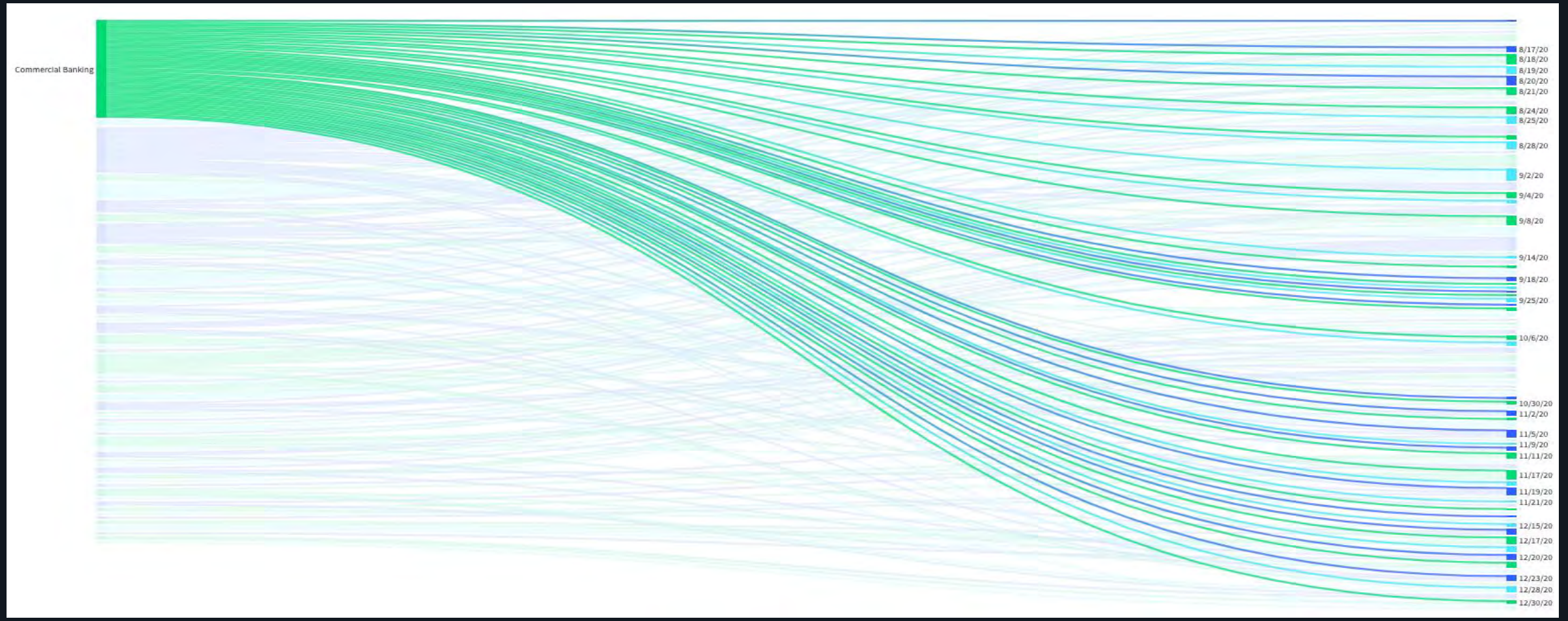
LBA Attacks

Late July to December 31, 2020



LBA Targeted Industries

Started Targeting Financial and Financial-adjacent Organizations



DDoS Attack Vectors used by LBA

DNS Reflection/Amplification is the preferred vector

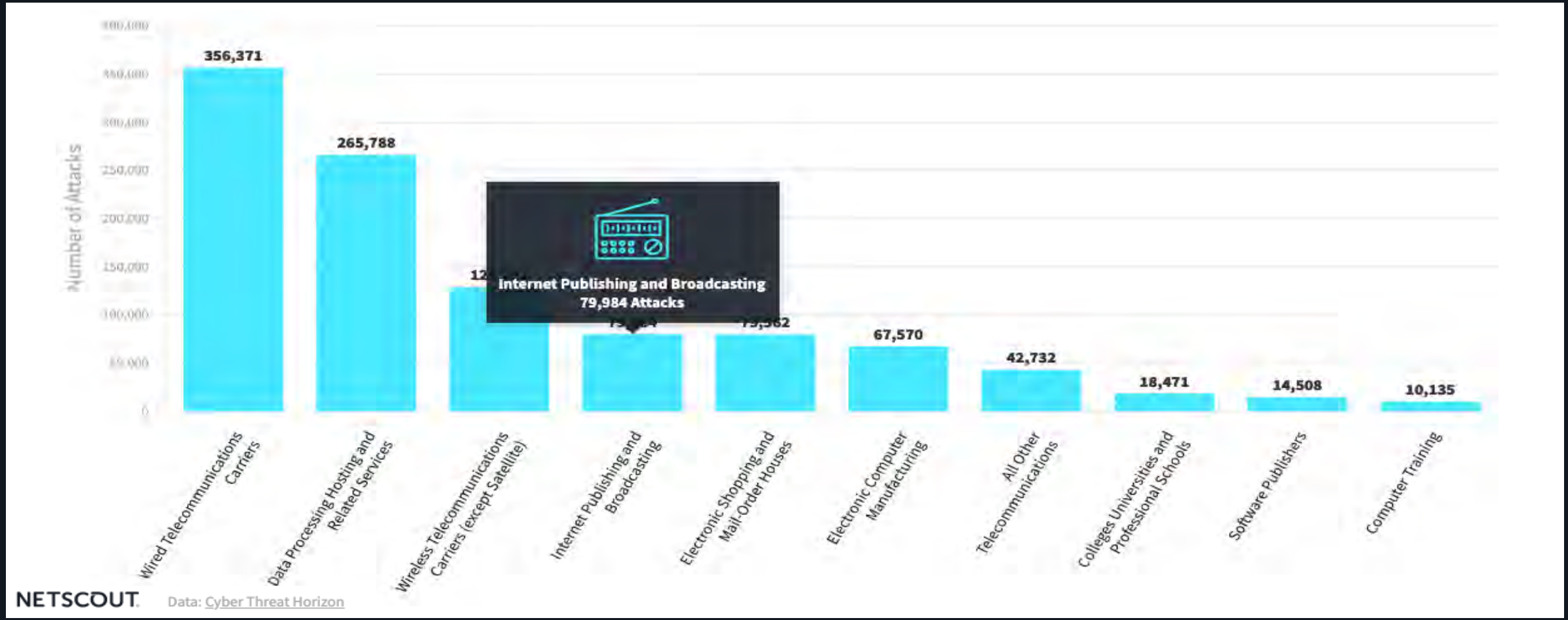
NETSCOUT

Top Vertical Industries Targeted

How Attack Target Selection Changed During the Pandemic

Top 10 Vertical Industry Targets

2H 2020



NETSCOUT

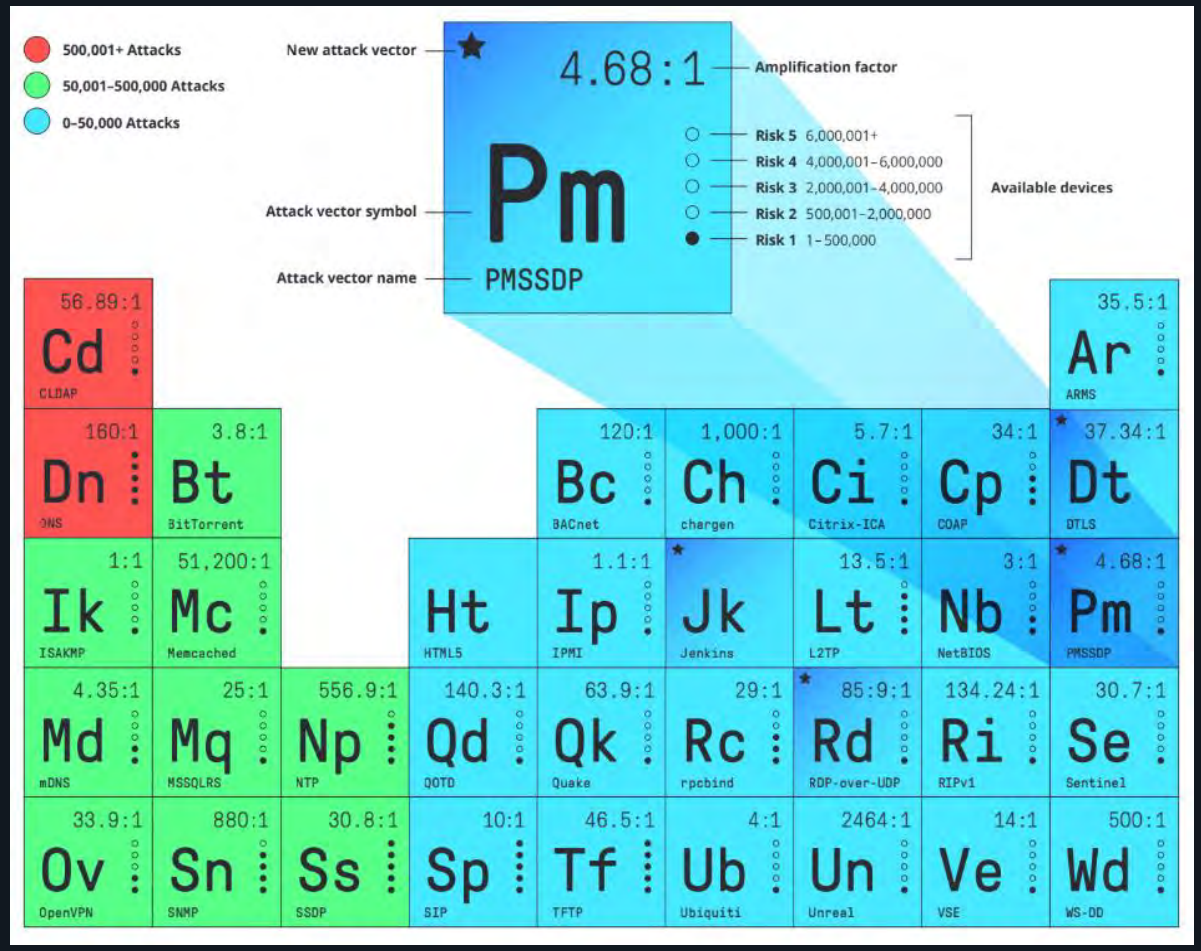
Emerging and Top DDoS Vectors

A Periodic Table of DDoS Attack Vectors

Periodic Table of DDoS Attack Vectors

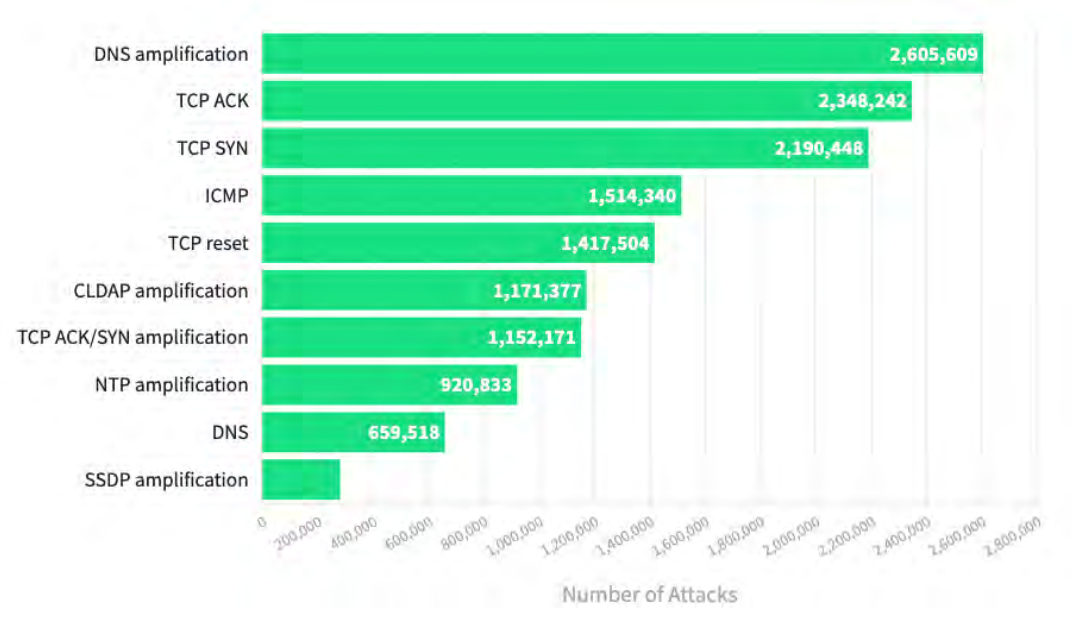
New DDoS Attack Vectors

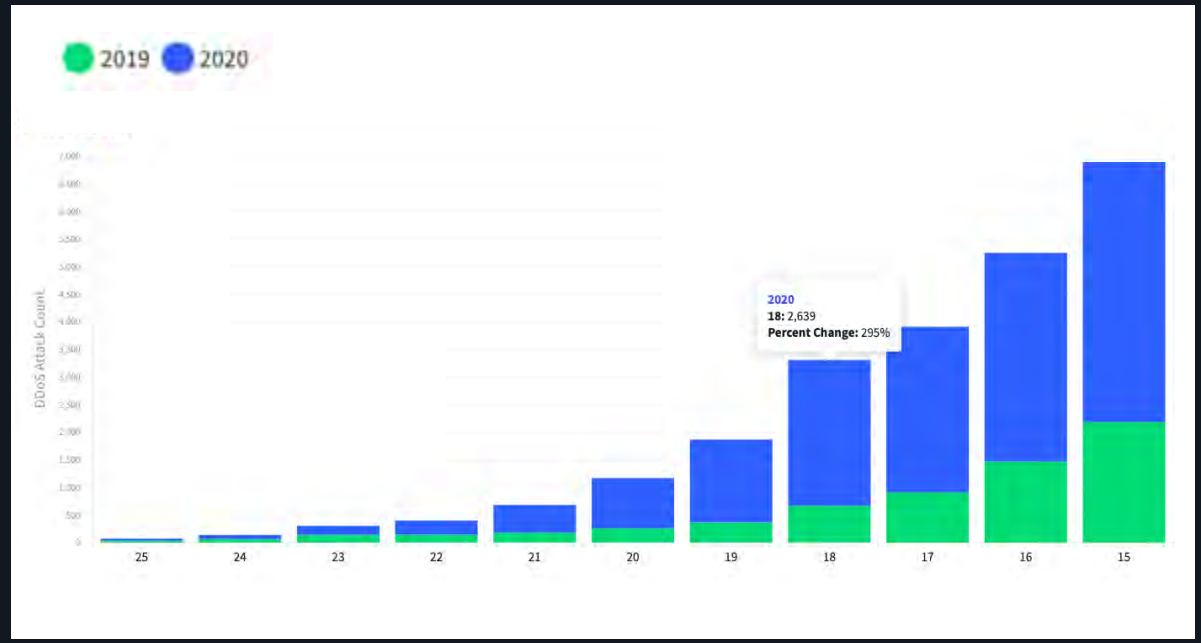
- RDP-Over-UDP (RDP)
  - 85.9:1 amplification ratio
  - Approx. 33k abusable reflectors
  - Attacks up to 750gb/sec
- Plex Media SSDP (PMSSDP)
  - 4.68:1 amplification ratio
  - Approx. 37k Abusable reflectors
- Data Transport Layer Security (D/TLS)
  - 37.34:1 amplification ratio
- Jenkins
  - A fizzle



Top DDoS Attack Vectors

2020 Review





- DNS reflection/amplification topped the charts
- TCP-based Floods remain a popular second

- Multi-vector DDoS attacks comprised of between 15–25 distinct vectors increased between 9% to 312% in 2020

NETSCOUT

Regional DDoS Attack Statistics

Attack Vectors, Volumes, and Throughput

Regional DDoS Attack Trends

2H 2020

- North America
  - 29% increase in frequency
  - Decreased attack duration
- Latin America
  - 50% increase in frequency
  - Decreased attack duration
- Europe, Middle East, & Africa
  - 33% increase in frequency
  - Decreased attack duration
- Asia Pacific
  - -8% decrease in Frequency
  - Decreased attack duration

DDoS Attack Coefficient (DAC) Bandwidth

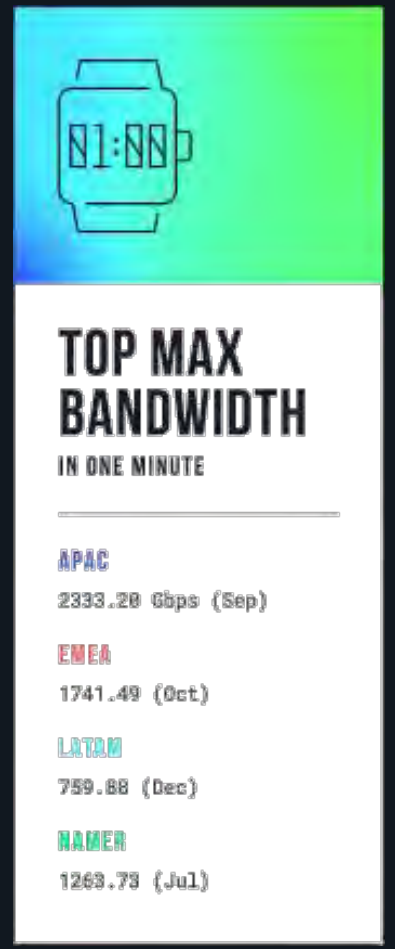
Regional Breakdown

- DAC represents the aggregate sum of attacks in one minute.

DDoS Attack Coefficient: Max Bandwidth

Month	APAC	EMEA	LATAM	NAMER	Regional Breakdown
Jul	774.11 Gbps	1997.13 Gbps	372.93 Gbps	1263.73 Gbps	
Aug	1486.81 Gbps	1440.46 Gbps	298.35 Gbps	764.94 Gbps	
Sep	2333.20 Gbps	1414.91 Gbps	575.01 Gbps	778.37 Gbps	
Oct	1282.53 Gbps	1741.49 Gbps	636.64 Gbps	627.40 Gbps	
Nov	1354.52 Gbps	1446.17 Gbps	591.92 Gbps	758.90 Gbps	
Dec	972.32 Gbps	1454.99 Gbps	759.88 Gbps	777.18 Gbps	

NETSCOUT Data: Cyber Threat Horizon



DDoS Attack Coefficient (DAC) Throughput

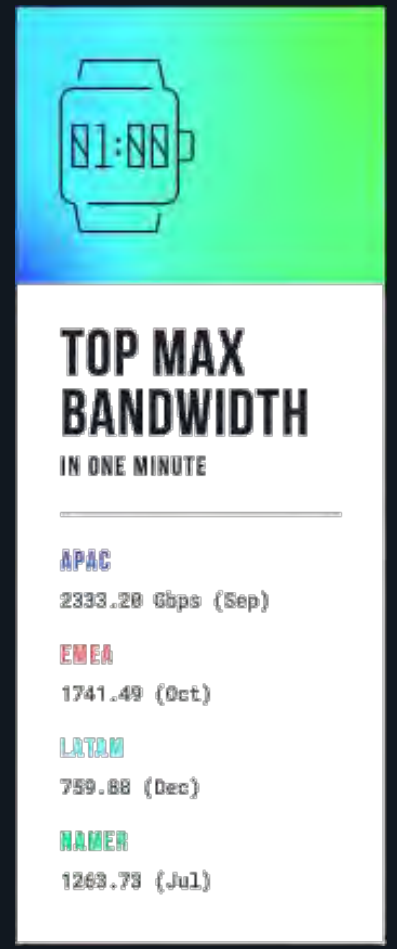
Regional Breakdown

- DAC represents the aggregate sum of attacks in one minute.

DDoS Attack Coefficient: Max Throughput

Month	APAC	EMEA	LATAM	NAMER	Regional Breakdown
Jul	474.23 Mpps	704.08 Mpps	74.97 Mpps	223.35 Mpps	
Aug	287.58 Mpps	544.21 Mpps	73.90 Mpps	200.91 Mpps	
Sep	1337.13 Mpps	523.45 Mpps	165.22 Mpps	167.06 Mpps	
Oct	822.93 Mpps	732.84 Mpps	171.57 Mpps	180.48 Mpps	
Nov	522.15 Mpps	560.87 Mpps	176.37 Mpps	256.84 Mpps	
Dec	360.81 Mpps	540.30 Mpps	211.77 Mpps	315.35 Mpps	

NETSCOUT Data: Cyber Threat Horizon

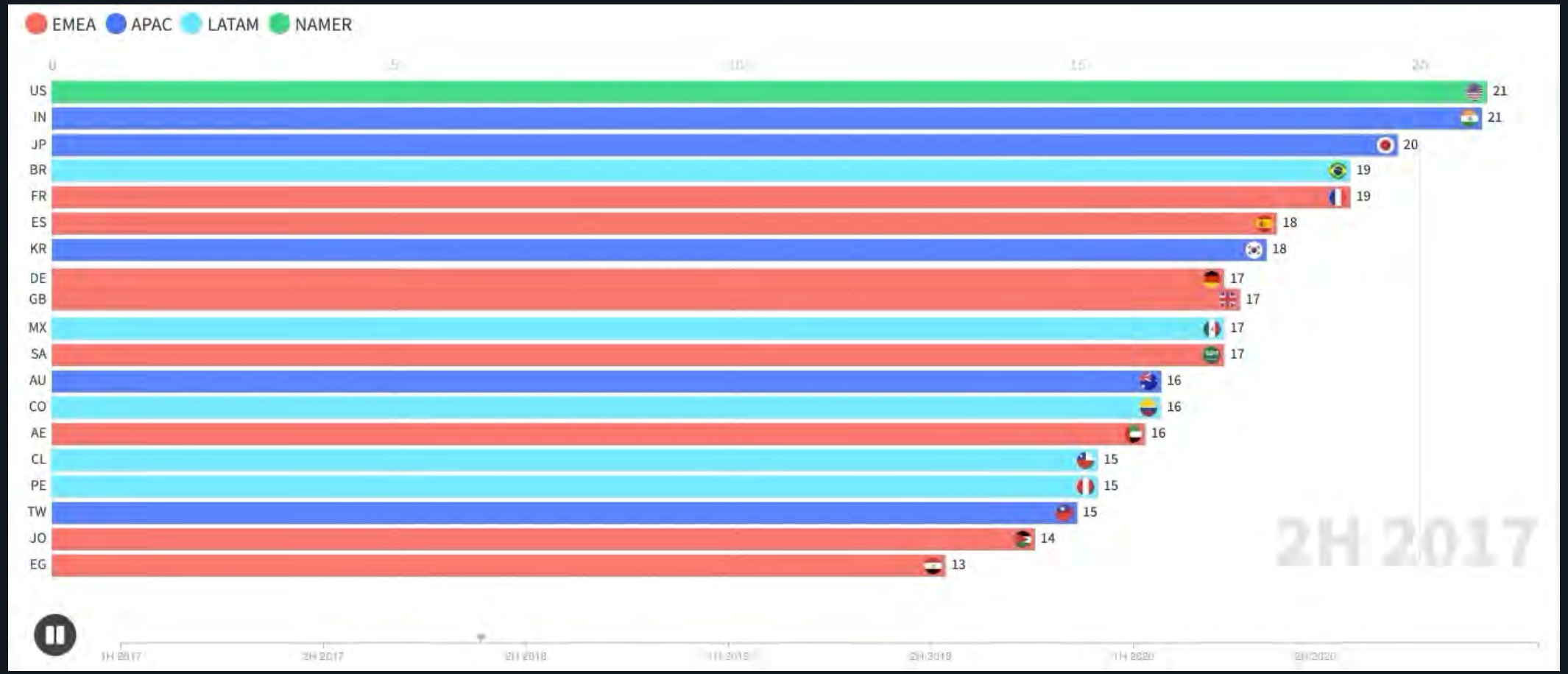


Regional Multi-Vector Attack Growth Since 2017

"Up and to the Right"

Multi-Vector Attacks by Country Since 2017

"Up and to the Right"



Country Snapshots

2H 2020

- Individual Statistics for 19 different countries.
- Highlights max attacks, attack vectors, and trends for the second half of 2020

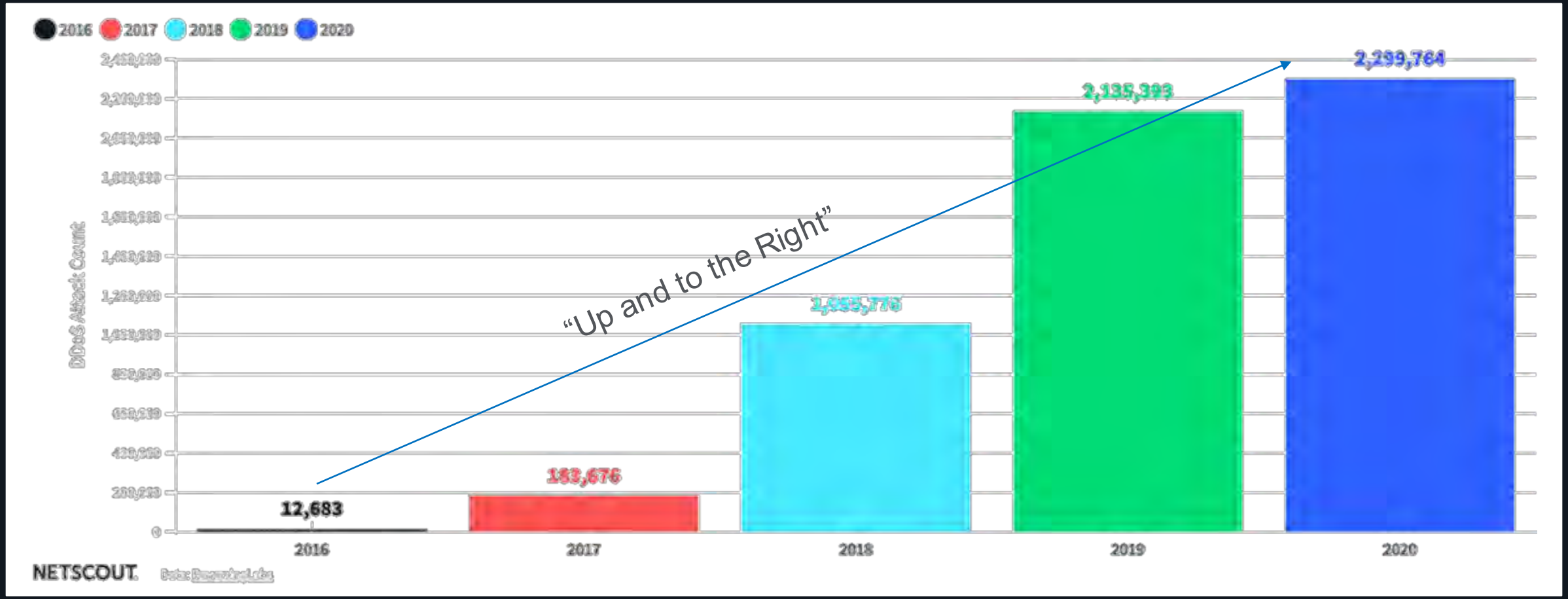
NETSCOUT

Internet of Things

Emergence of a New Botnet

Mirai: Long Live the King

Data Provided by ReversingLabs



Brute-Force IoT Exploitation

Remains the #1 Method of IoT Bot Propagation

- Unique sources indicate non-mirai passwords lists in circulation (left)
- Summary of brute-force attempts illustrate the persistent nature of Mirai (right)

Top Five Username/Password Combinations by Unique Source

	Username/Password	Unique Sources
1	guest/12345	110,467
2	root/xc3511	98,933
3	admin/admin	90,592
4	root/vizxv	76,392
5	root/root	62,518

NETSCOUT

Top Five Username/Password Combinations by Total Attempts

	Username/Password	Total Attempts
1	root/xc3511	5,161,000
2	admin/	3,273,127
3	root/icatch99	2,146,214
4	default/default	1,578,778
5	default/	1,409,367

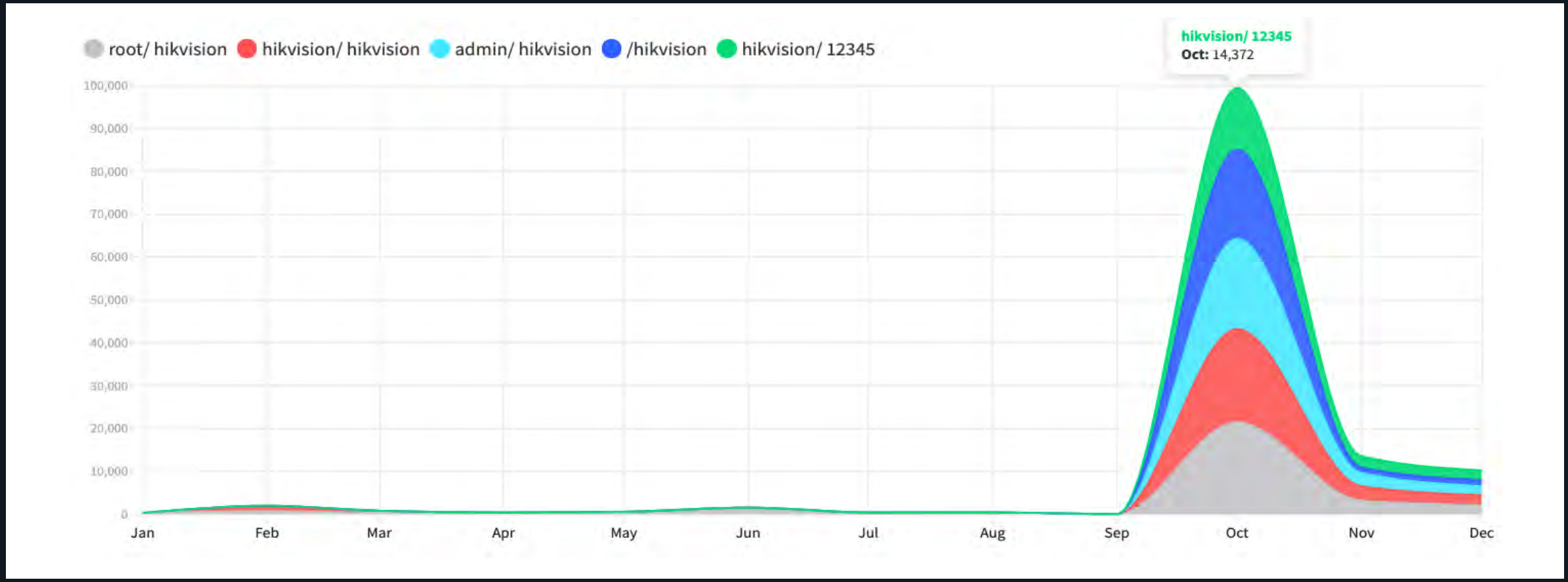
NETSCOUT

A View of Telnet Activity – 2H 2020

Victim and Attacker Top 50 Countries

A Disturbance in the Force

Emergence of a New Botnet



Free DDoS Resources for the Operational Community

2020 Threat Report

https://www.netscout.com/threatreport

Ongoing DDoS Attack Statistics and Trends

https://horizon.netscout.com

Thank You!

A Year Like No Other

DDoS in a Time of Pandemic

Roland Dobbins <roland.dobbins@netscout.com>

Principal Engineer, ASERT

netscout.com