Telia Carrier

DDoS THREAT LANDSCAPE REPORT 2021

EXECUTIVE SUMMARY

DDOS ATTACKS CONTINUE TO INCREASE, WITH EVER GREATER NETWORK IMPACT – THE LARGEST ATTACK IN 2020 HIT 1.18 TBPS – UP 50% FROM THE PREVIOUS YEAR

INCREASE MIRRORS THE MAIN WAVES OF THE PANDEMIC

- We saw a natural increase in mitigated traffic during 2020 – consistent with greater customer adoption of our DDoS protection service, but we also observed more attacks targeting our customers in general. These appear to have mirrored the main waves of the pandemic and periods during which harder lockdown restrictions were imposed in many countries worldwide. We believe this was largely opportunistic, as cybercriminals took advantage of a sudden shift to remote working & learning.

MORE MULTI-VECTOR ATTACKS AND EXTORTION THREATS

- Customers didn't just feel the pain of more attacks but had to deal with more multi-vector attacks to boot – fueling greater reliance on auto-mitigation. Our IP customers also experienced a significant increase in threats and extortion-based attacks. This can be partly attributed to the pandemic, as companies suddenly became more dependent on cloud workflows and remote systems (and subsequently more vulnerable).

NUMBER OF ATTACKS IS PROPORTIONAL TO SIZE OF CUSTOMER BASE

- Geographically speaking there was a direct relationship between the size of our IP customer base and the overall number of attacks across different regions – more customers meant more DDoS.

DNS & NTP AMPLIFICATION

- DNS and NTP amplification attacks were the most common attack vector in 2020. Average packet length increased during 2020 and attack vectors have shifted from small packet SYN attacks to larger packet attacks with amplification.

CARPET BOMBING BECAME MORE FREQUENT AND IS HERE TO STAY

KEY FINDINGS

MORE ATTACKS AND A GREATER NETWORK IMPACT

DDoS attacks continue to increase, with ever greater network impact – the largest attack in 2020 hit 1.18 Tbps - up 50% from the previous year.

ATTACK DISTRIBUTION REFLECTS MARKET PRESENCE

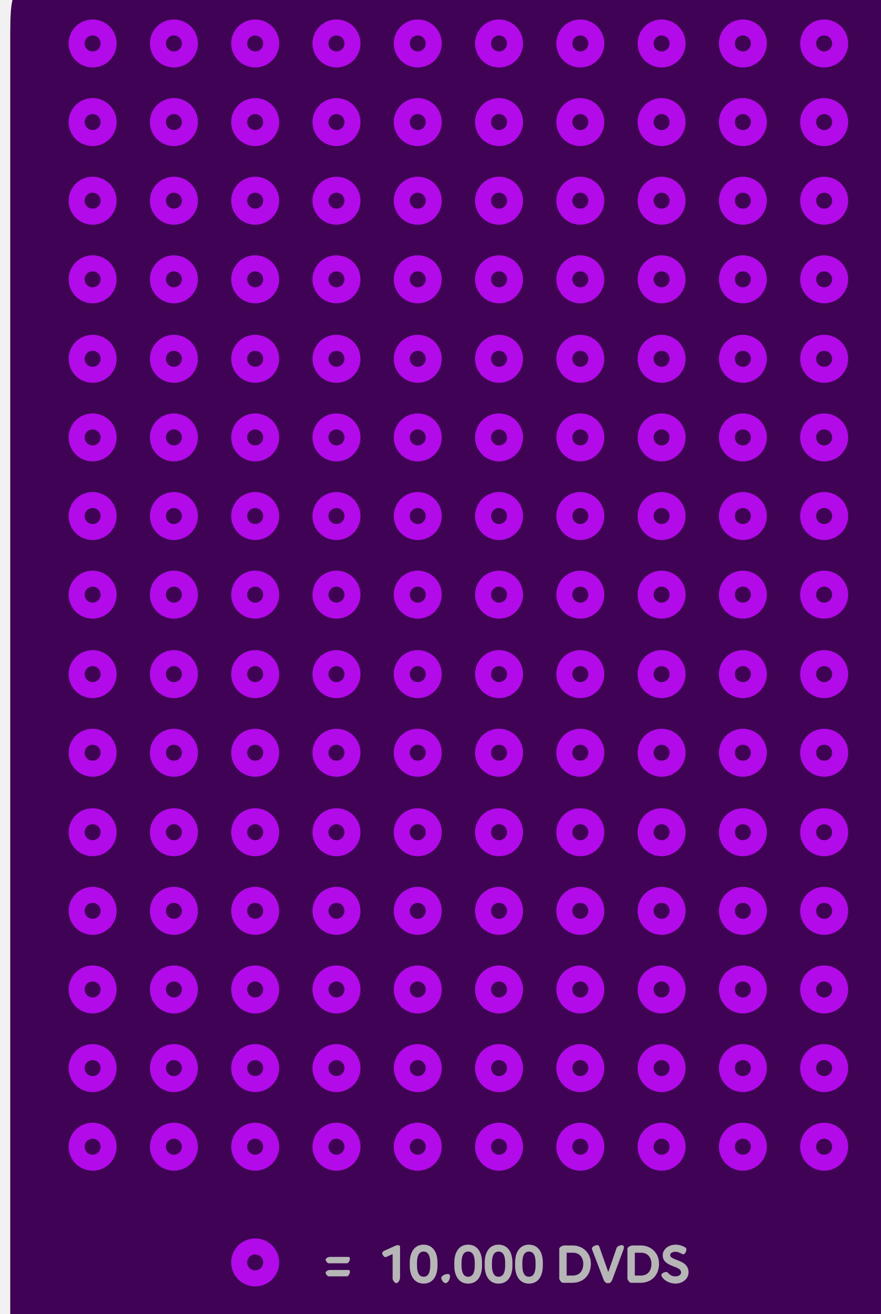
Geographically, DDoS attack distribution directly reflected our market presence in different regions, with more attacks where we connect the most customers.

GREATER INCIDENCE OF HIGH-INTENSITY PACKET-PER-SECOND ATTACKS

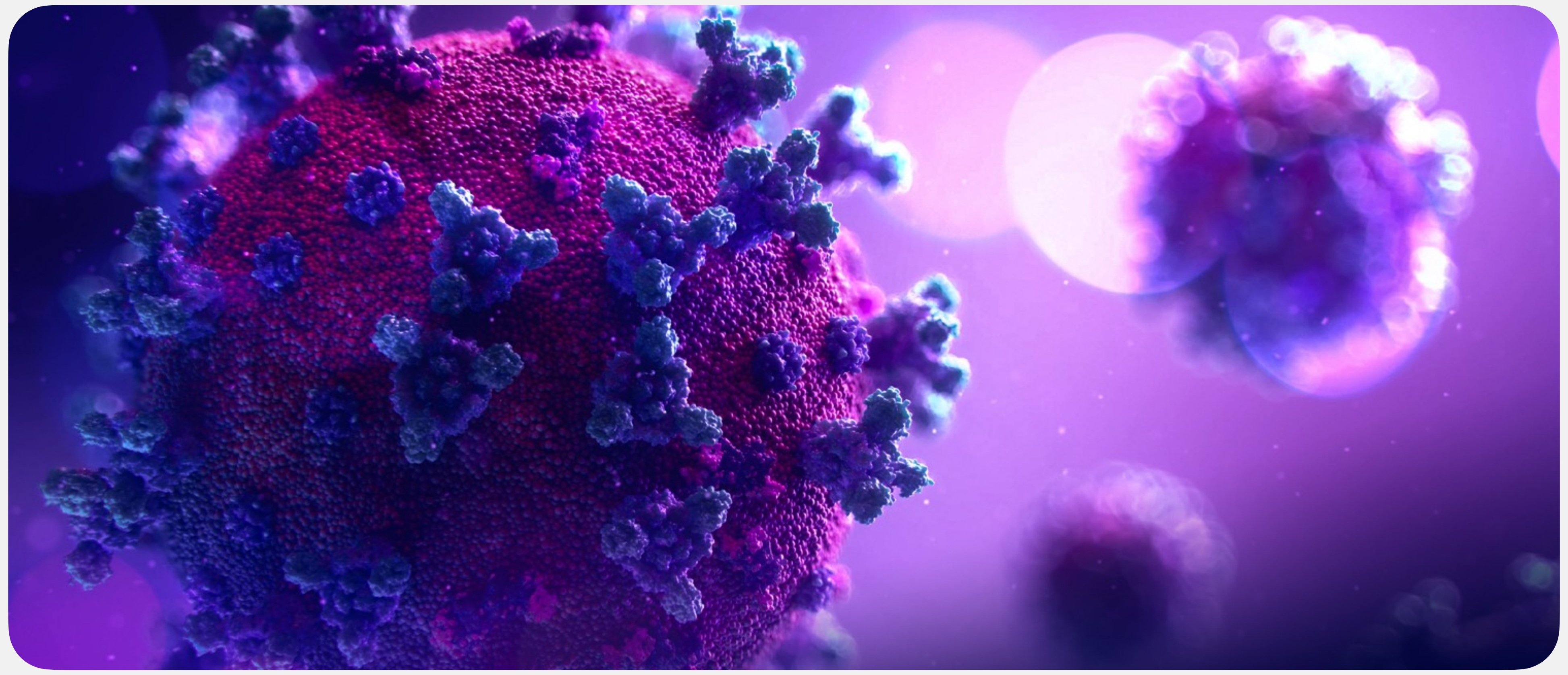
In terms of packets-per-second, the size of the largest attack reached 887 Mpps. With an increase in available network capacity overall, cyber-criminals are increasingly targeting their victims with high-intensity packet-per-second attacks, rather than simply congesting client links.

INCREASING CUSTOMER UPTAKE RESULTED IN MORE SCRUBBING

We cleaned 57 petabits of malicious data and 14 x 1012 packets – the equivalent of 1.5 million DVDs.



SCRUBBED THE EQUIVALENT OF 1.5 MILLION DVDS OF MALICIOUS DATA



ACTIVITY PEAKS MIRROR COVID LOCKDOWNS

There was a significant ‘Covid-effect’, with an overall increase in attacks and activity peaks that appear to have mirrored the main spring and autumn lockdown waves in the US and Europe.

CUSTOMER ATTACKS INCREASED IN BOTH FREQUENCY & DURATION

THE AVERAGE SIZE OF EACH ATTACK WAS 19 GBPS OR 23 MPPS

THE AVERAGE DURATION OF EACH ATTACK WAS APPROXIMATELY 10 MIN

ATTACK VECTORS HAVE SHIFTED FROM SMALL PACKET SYN ATTACKS TO LARGER PACKET ATTACKS WITH AMPLIFICATION

A TREND TOWARDS AUTO-MITIGATION OF ATTACK TRAFFIC

Due to an increase in multi-vector attacks, customers are moving towards auto-mitigation of attack traffic.

CUSTOMERS REQUIRE A REVISED APPROACH TO DETECTION AND MITIGATION

Carpet bombing has become more commonplace & frequent, placing an increasing strain on customer network infrastructure. This requires a revised approach to traditional threshold-based detection and mitigation (from host-level to logical network-level.

DNS AND NTP AMPLIFICATION ATTACKS WERE THE MOST COMMON ATTACK VECTOR IN 2020

AVERAGE ATTACK PACKET LENGTH INCREASED DURING 2020

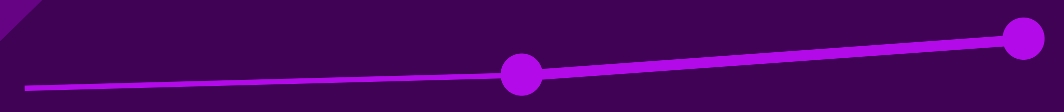
BREAKDOWN OF FINDINGS

OVERALL NETWORK IMPACT

PEAK ATTACK GBPS (LY) *

1.18
TBPS

↗ 49.37%



PEAK ATTACK MPPS (LY) *

887
MPPS

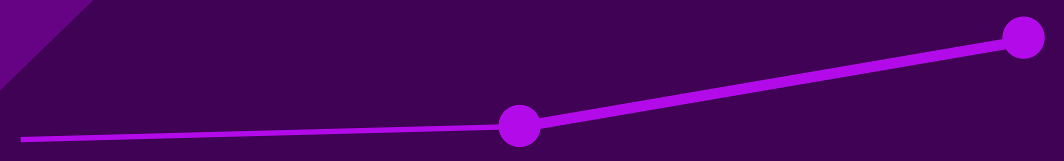
DDOS ATTACKS CONTINUE TO INCREASE – IN SIZE AND SCALE, AND WITH EVER GREATER NETWORK IMPACT

MITIGATION VOLUME

CLEANED PETABITS (LY)

57 PB

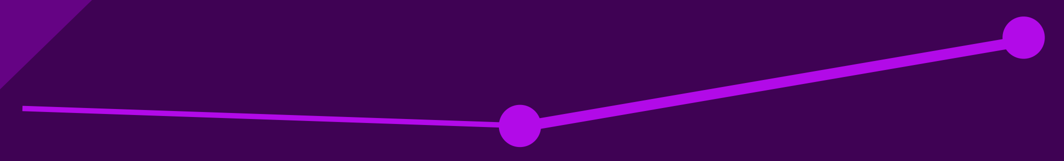
↗ 192%



CLEANED TERA PACKETS (LY)

14 TP

↗ 176%



WE CLEANED 57 PETABITS AND 14 TERA PACKETS OF MALICIOUS DATA IN 2020 – THE EQUIVALENT OF 1.5 MILLION DVDS

AVERAGE ATTACK SIZE & DURATION

DDOS ATTACK AVG SIZE GBPS (LY)

19
GBPS

DDOS ATTACK AVG SIZE MPPS (LY)

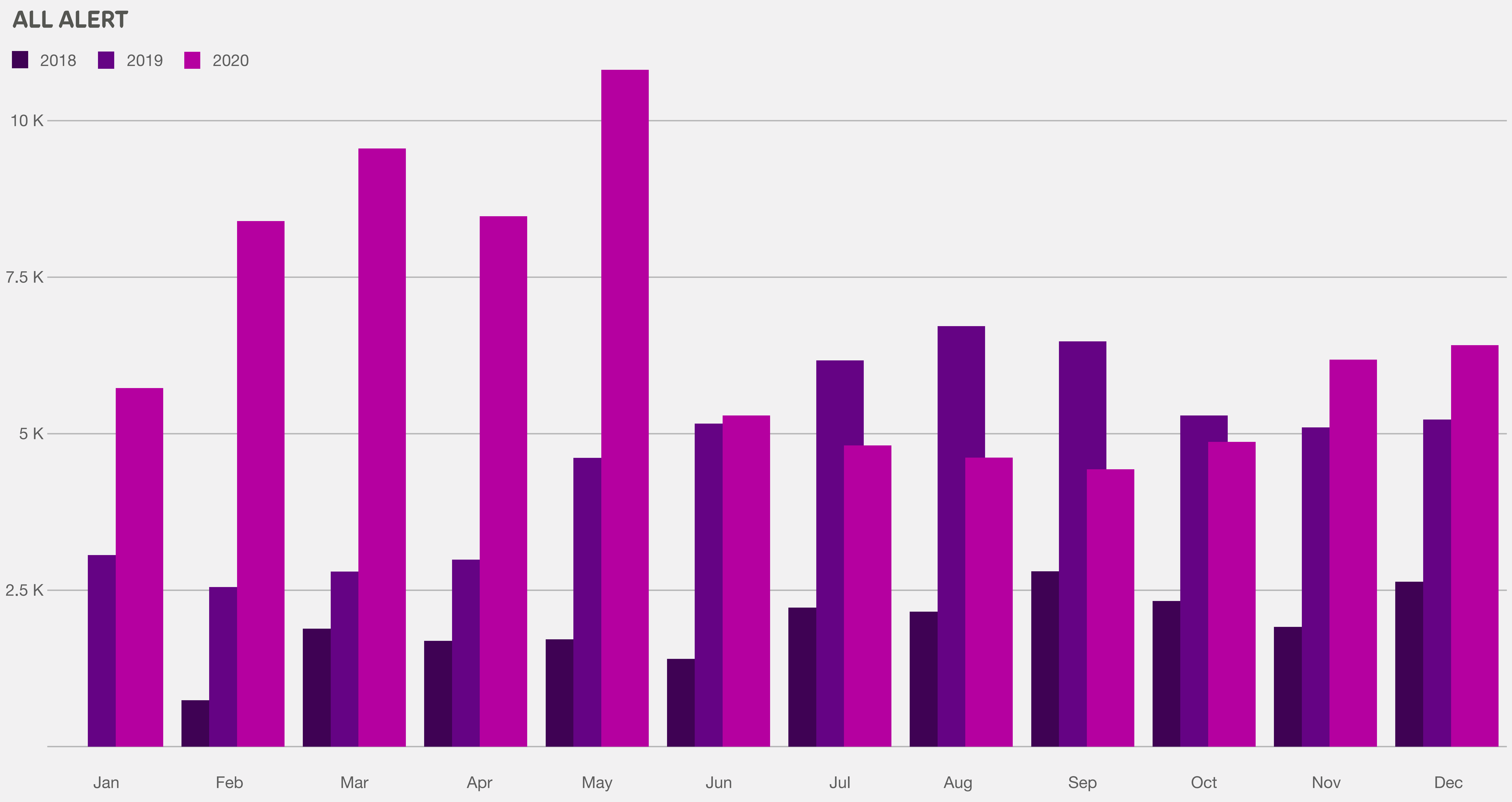
23
MPPS

DDOS ATTACK AVG DURATION (LY)

10
MIN

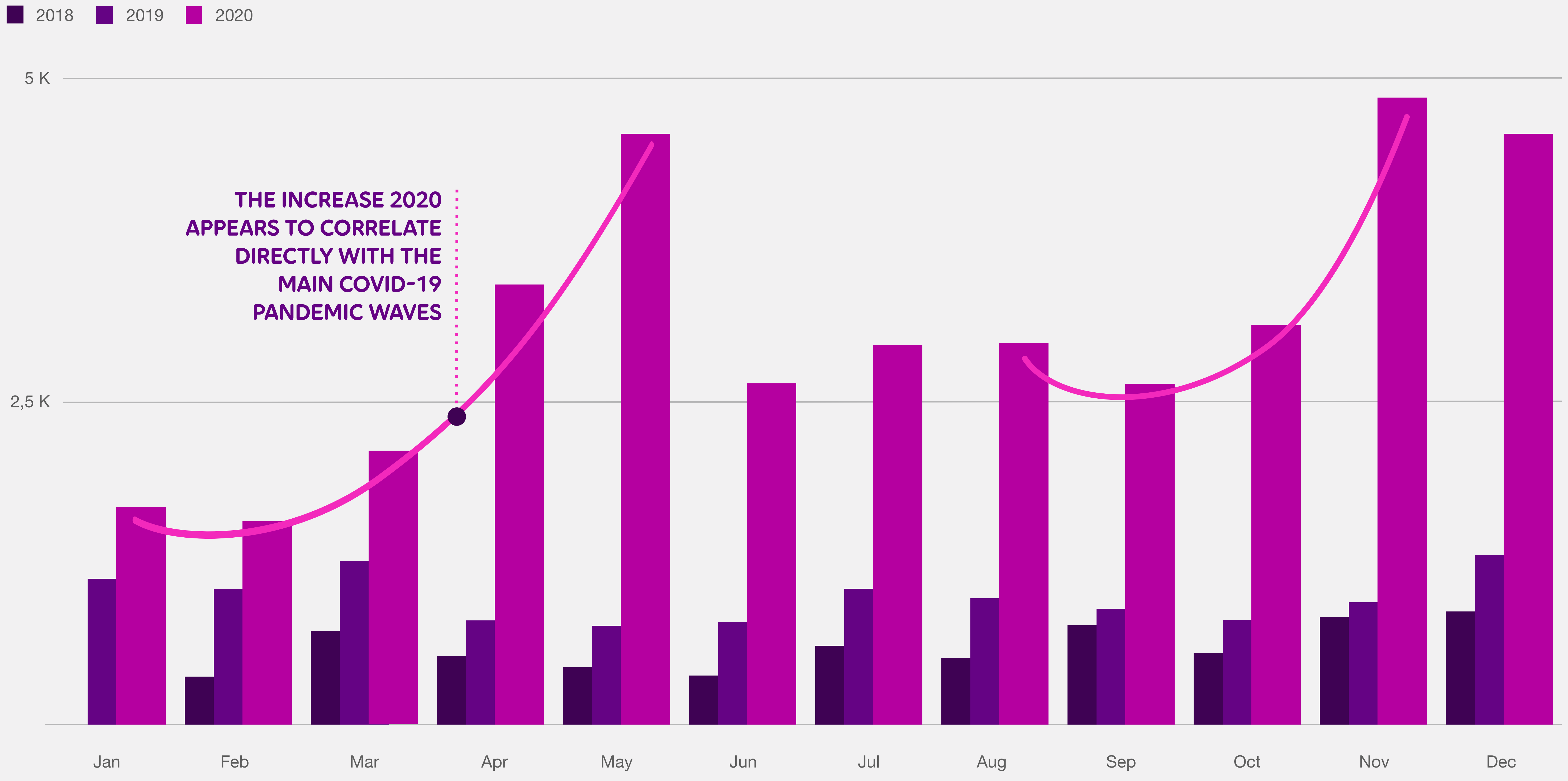
ATTACK FREQUENCY AND DURATION

THE NUMBER OF EXTREME (TOP 10% BY SIZE) ATTACKS INCREASED DURING H1 2020 BUT TAILED-OFF LATER IN THE YEAR



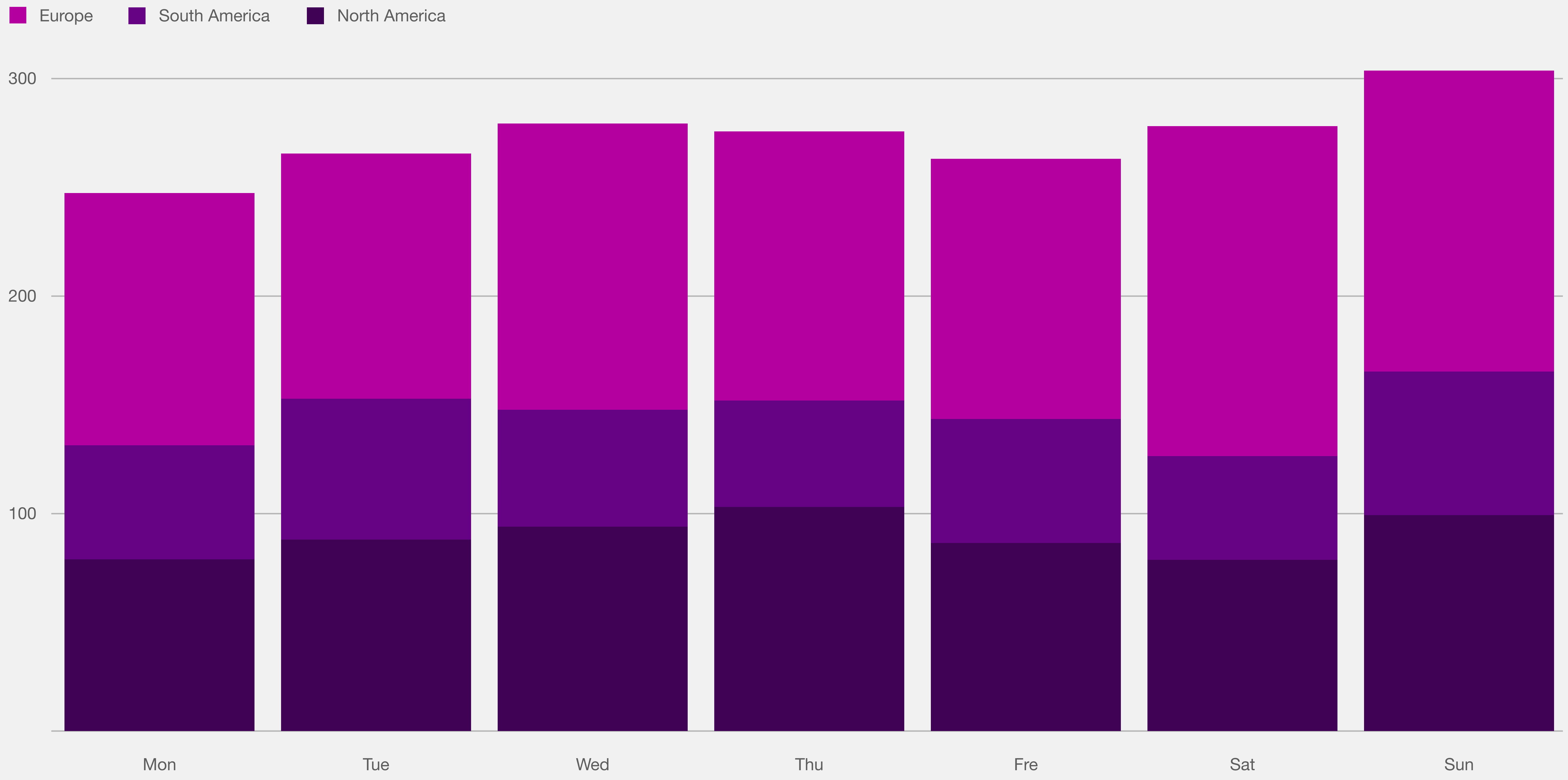
WE NOTICED A DRAMATIC INCREASE IN ATTACKS TARGETING CUSTOMERS WITH OUR DDOS PROTECTION SERVICE STARTING IN MARCH/APRIL AND THROUGHOUT 2020

DDOS SERVICE ALERT



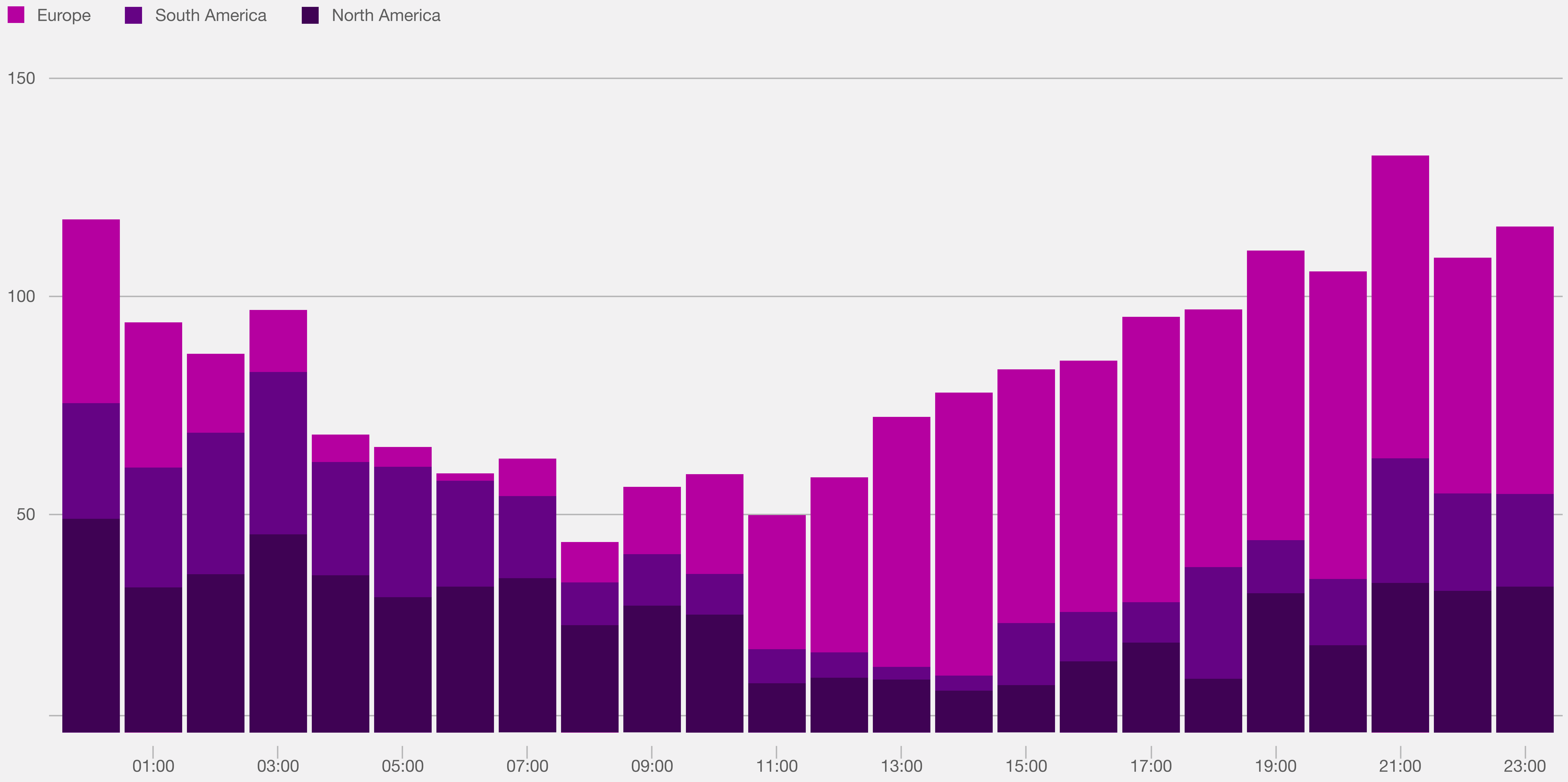
ATTACKS WERE CONSTANT AND AFFECTED CUSTOMERS THROUGHOUT THE WEEK. "YOU ARE NEVER SAFE"

DDOS CUSTOMER CONTINENT WEEKDAY (LY)

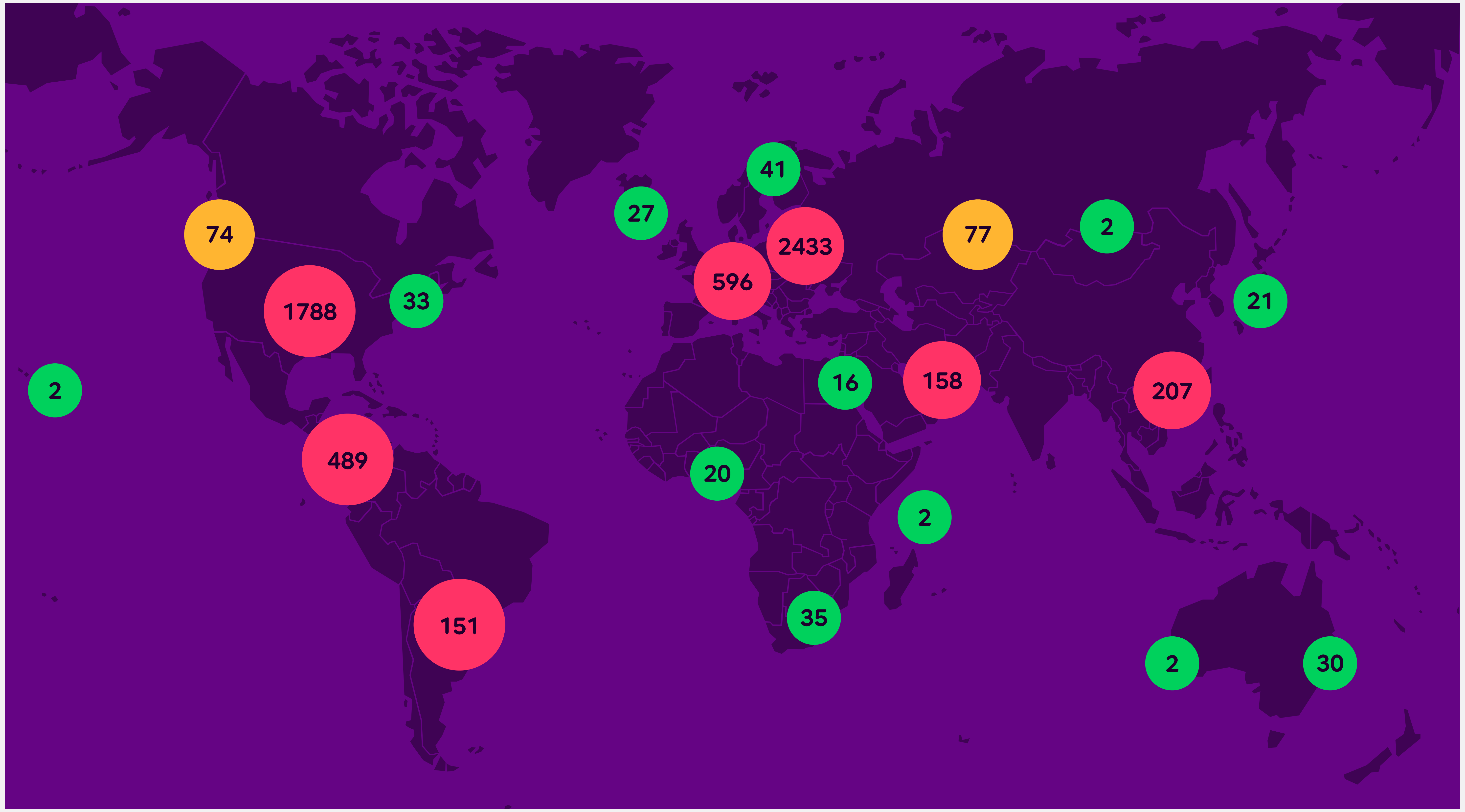


ATTACKS TENDED TO ‘FOLLOW THE SUN’ ACROSS DIFFERENT CONTINENTS

DDOS CUSTOMER CONTINENT HOUR (LY)



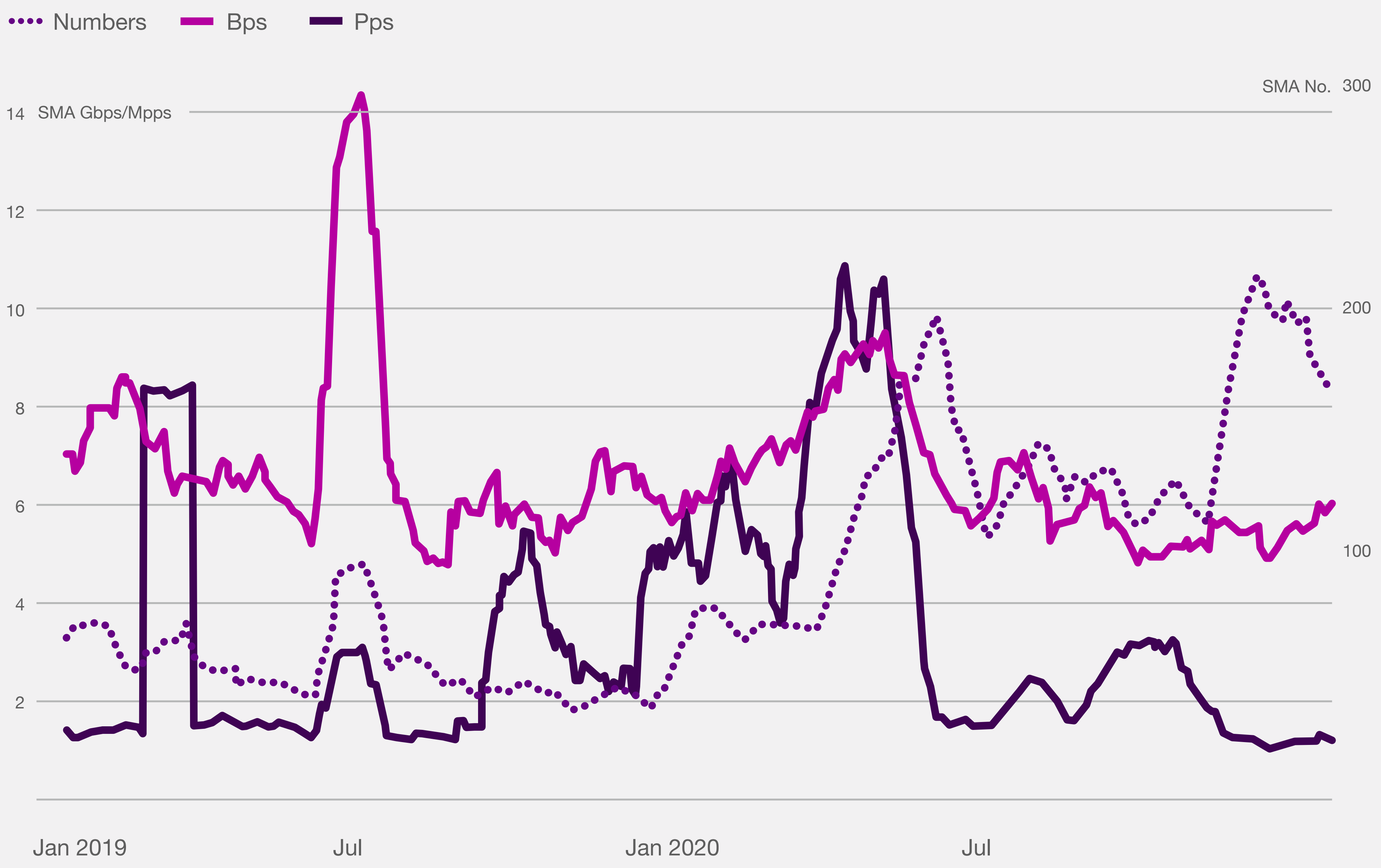
GEOGRAPHICAL DISTRIBUTION



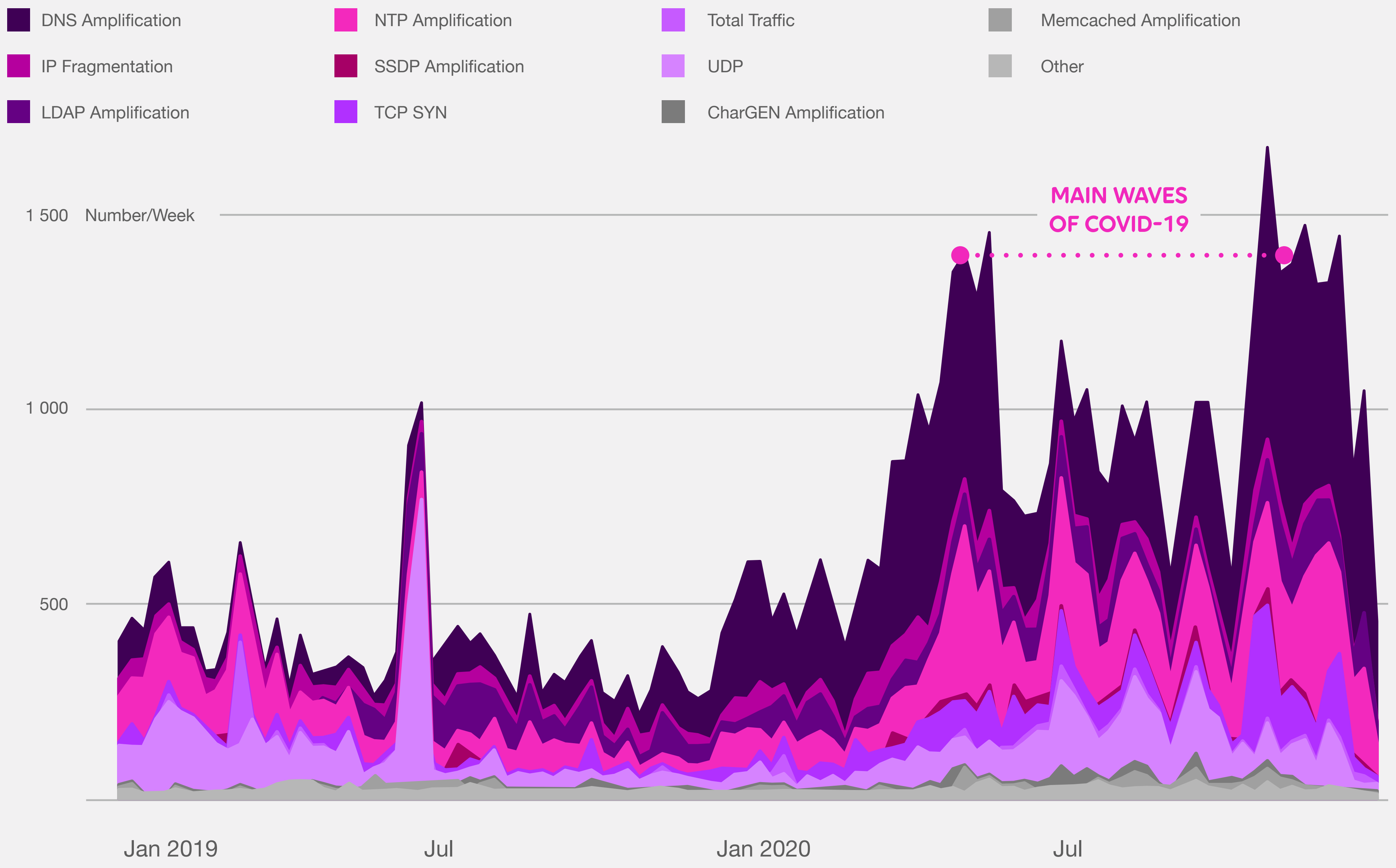
WE SAW THE HIGHEST CONCENTRATION OF DDOS ATTACKS IN OUR KEY MARKETS, REFLECTING GREATER OVERALL CUSTOMER NUMBERS TRAFFIC

CUSTOMER ATTACK TRENDS

ATTACK SIZE DDOS CUSTOMER PER DAY (2 LY)



ALERT TYPES DDOS CUSTOMER PER WEEK (2 LY)

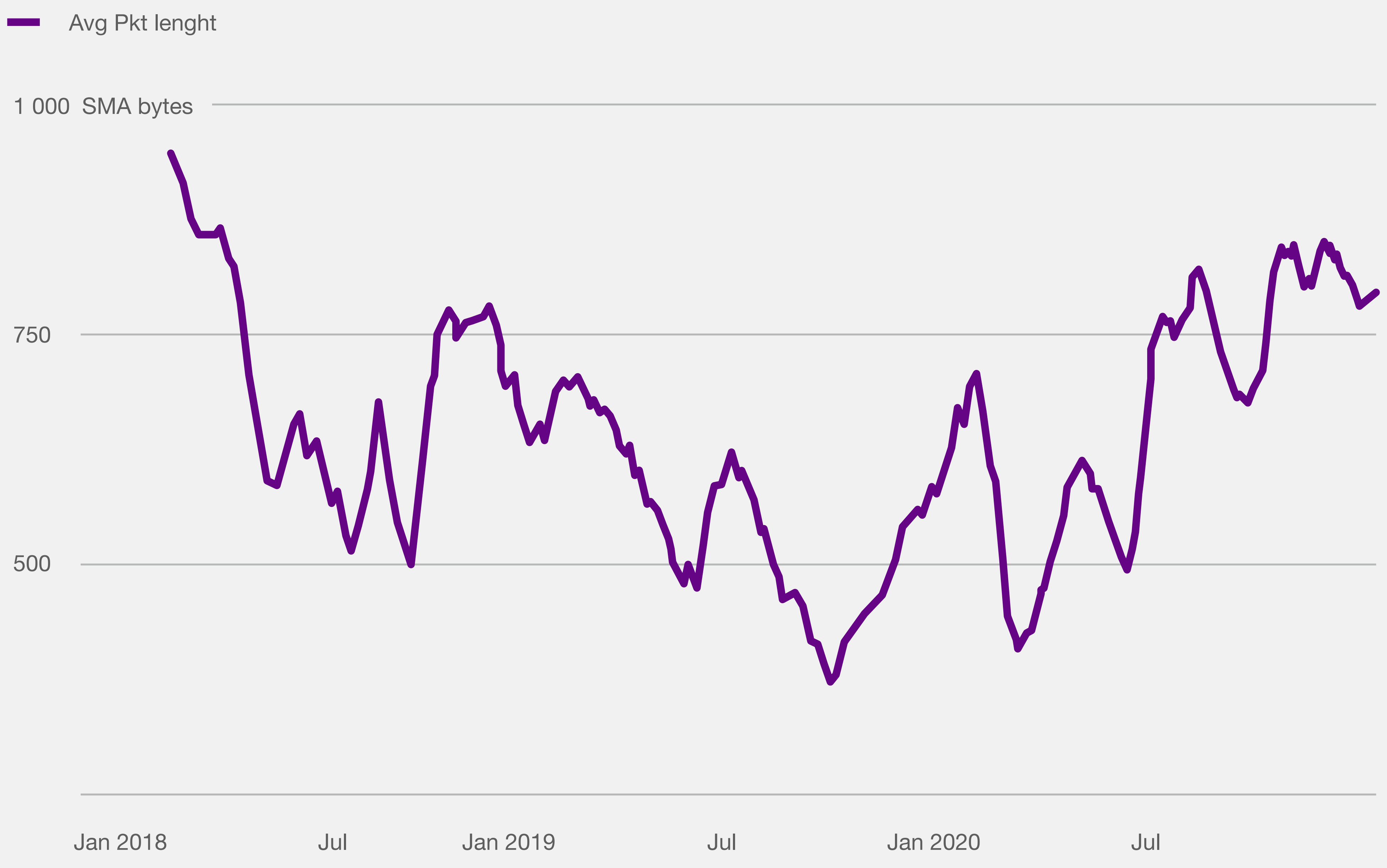


THERE APPEARS TO BE A DISTINCT CORRELATION BETWEEN THE TWO MAIN PANDEMIC WAVES (LOCKDOWN PHASES) AND THE NUMBER OF DDOS ATTACKS TARGETING OUR CUSTOMERS

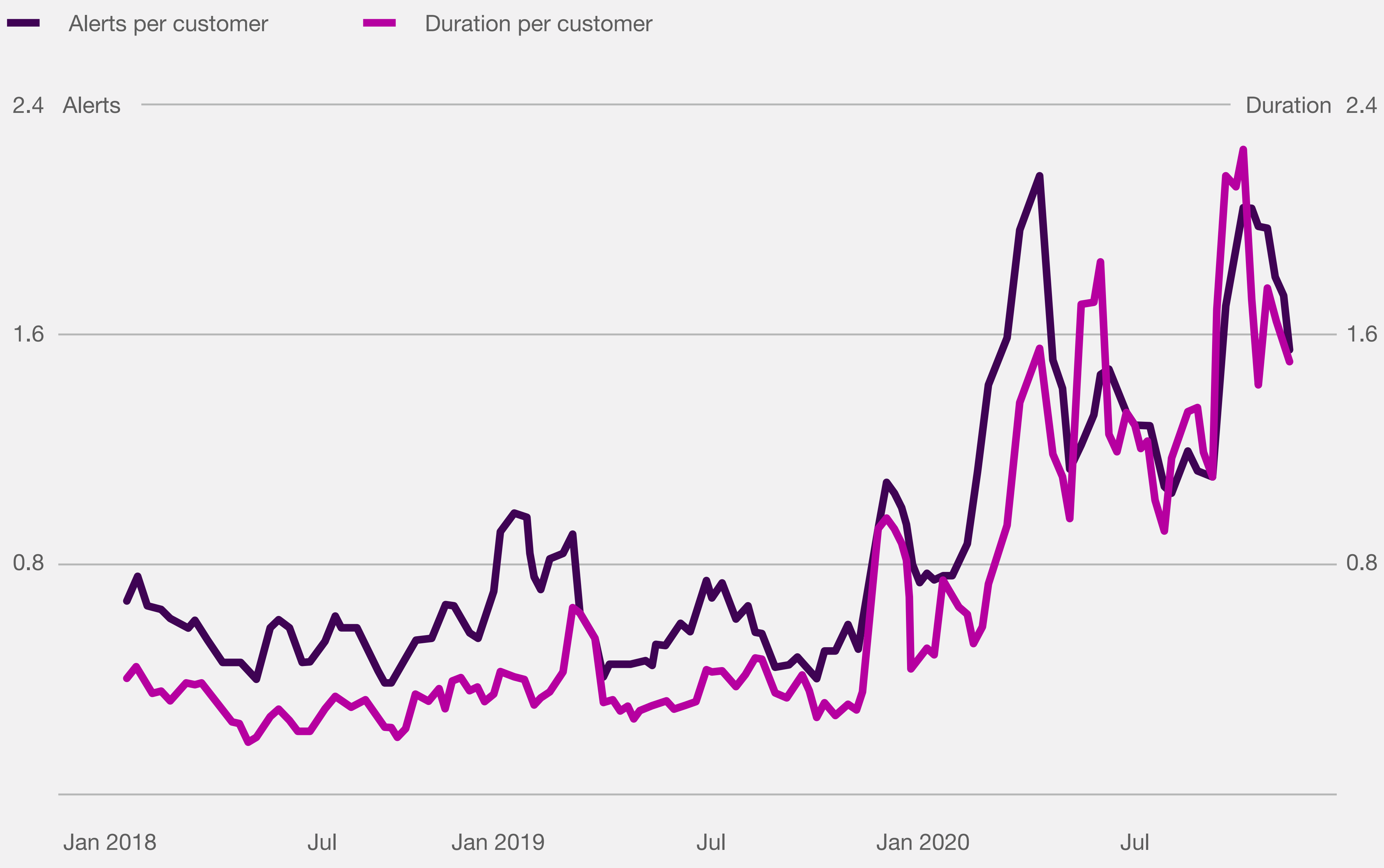
DNS & NTP AMPLIFICATION WERE THE MOST COMMON TYPES OF ATTACK IN 2020

SCALE AND INTENSITY

ATTACK AVG PKT LENGHT PER DAY (3 LY)



ALERTS & DURATION PER DDOS CUSTOMER (3 LY)



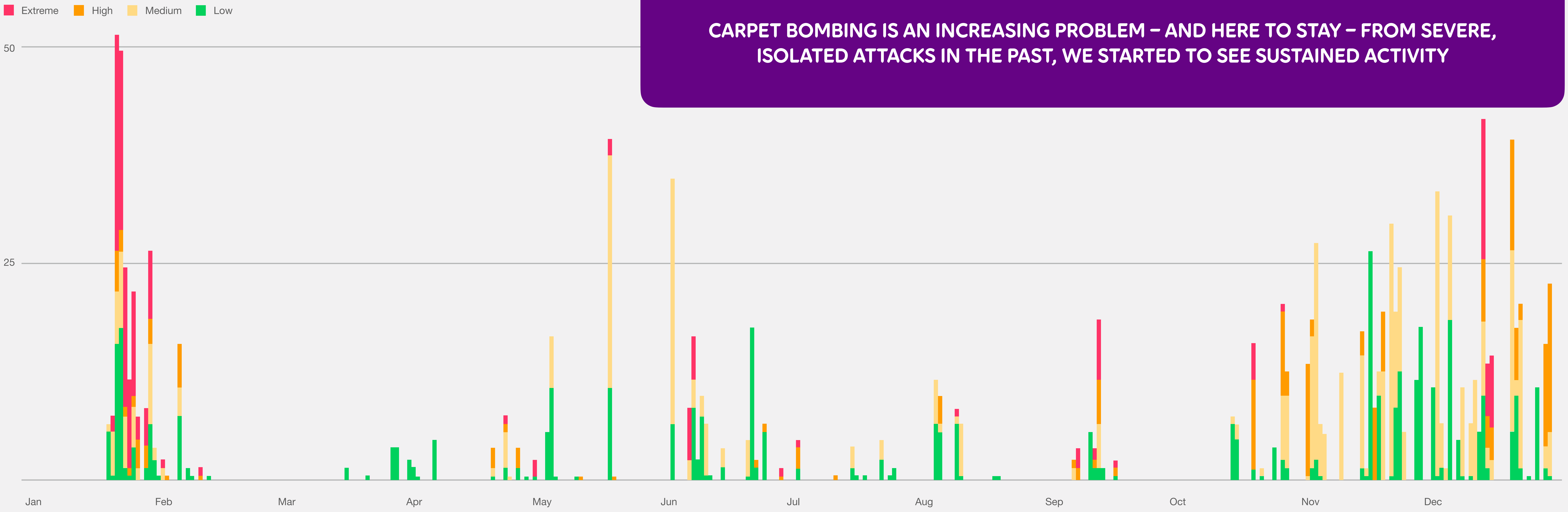
AVERAGE PACKET LENGTH INCREASED THROUGH 2020

ATTACK VECTORS SHIFTED FROM SMALL PACKET SYN ATTACKS TO LARGER PACKET ATTACKS WITH AMPLIFICATION

OVERALL, CUSTOMERS EXPERIENCED MORE ATTACKS, WITH LONGER DURATION DURING 2020

CARPET BOMBING

GLOBAL CARPET BOMBING SEVERITY (LY)



CARPET BOMBING IS AN INCREASING PROBLEM – AND HERE TO STAY – FROM SEVERE, ISOLATED ATTACKS IN THE PAST, WE STARTED TO SEE SUSTAINED ACTIVITY

ABOUT TELIA CARRIER

Telia Carrier solves global connectivity challenges for multinational enterprises whose businesses rely on digital infrastructure. On top of the world's Number-1-ranked IP backbone and a unique ecosystem of cloud and network service providers, we provide an award-winning customer experience to customers in 125 countries worldwide.

Our global Internet services connect more than 700 cloud, security and content providers with low latency. For further resilience, our private Cloud Connect service connects directly to Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud and Oracle cloud across North America, Europe and Asia.

TELIACARRIER.COM/KNOWLEDGE-HUB

TELIACARRIER.COM

Telia Carrier