ISSUE 6: FINDINGS FROM 2H 2020

NETSCOUT THREAT INTELLIGENCE REPORT

Service Providers Battle DDoS in a Time of Pandemic

With internet connectivity a vital pandemic lifeline, CSPs were essential workers in 2020

DOUBLE WHAMMY FOR CSPS: AS NETWORK TRAFFIC SPIKES, SO DO DDOS ATTACKS

According to the latest NETSCOUT Threat Intelligence Report, communications service providers (CSPs) managed enormous spikes in legitimate network traffic while simultaneously defending a huge bump in DDoS attacks targeting critical network infrastructure and their customers.

NUMBER OF ATTACKS 2020

10,089,687

▲ **20%** Increase in attack frequency year over year

▲ **22%** Increase in attack frequency during the last six months

NEARLY 130,000 MORE ATTACKS PER MONTH IN 2020 ON AVERAGE

Record-breaking global DDoS attack stats

MAX ATTACK SIZE
1.12 Tbps

MAX THROUGHPUT
581 Mpps

LARGEST REGIONAL ATTACK FREQUENCY
3,753,883

AVERAGE GLOBAL ATTACK DURATION
39.83 Min

Use of OTT services skyrockets

41% of service providers were concerned with bandwidth saturation increases from pandemic-staple over-the-top (OTT) services such as streaming video, conference calls, and gaming.

Demand surges for managed DDoS protection services

69% Managed Security Service Providers faced a 69% increase in demand for managed DDoS protection services from companies of all sizes.

RECORD DDOS ATTACKS DRIVE INCREASED SP CONCERN

of service providers tap DDoS attacks as the top threat and concern

CSPs as Top Three industry targets

WIRELESS TELECOMMUNICATIONS CARRIERS	356,371
WIRED TELECOMMUNICATIONS CARRIERS	265,788
DATA PROCESSING HOSTING AND RELATED SERVICES	128,681

Attack complexity on the rise

Service providers expressed growing concern over the increasing complexity of attacks. Thanks to IoT botnets, reflection/amplification techniques, and DDoS-for-hire services, attacks are more distributed, complex, and powerful than ever before.

57% of service providers reported multivector attacks in 2020.

15+ Multivector DDoS attacks using 15-plus attack vectors soared.

26 vectors deployed in a single attack in 2020—the highest number yet seen.

DDoS traffic impacted operator networks worldwide

This was a record-breaking year for DDoS attacks—and that has to have an impact on global infrastructure, particularly since DDoS attackers don't pay for transit costs.

The DDoS Attack Coefficient (DAC) shows just how much aggregate DDoS traffic crosses internet pipelines in any given minute of time—essentially, the "DDoS tax" that we all end up paying.

MAX BANDWIDTH

APAC	2,330 Gbps (Sep)
EMEA	1,741.49 Gbps (Oct)
LATAM	759.88 Gbps (Dec)
NAMER	1,263.73 Gbps (Jul)

GLOBAL DDOS EXTORTION CAMPAIGN STRIKES SERVICE PROVIDERS

A group known as Lazarus Bear Armada launched one of the most sustained and extensive DDoS extortion campaigns yet seen.

Service providers in the crosshairs

Major targets included communications service providers and internet service providers.

Infrastructure targets

LBA used network reconnaissance to launch multivector attacks against not only applications and services, but also network and remote-access infrastructure elements.

- PEERING AND CUSTOMER AGGREGATION ROUTERS OF UPSTREAM ISPS
- VPN CONCENTRATORS
- AUTHORITATIVE AND RECURSIVE DNS SERVERS

AS THE COVID-19 PANDEMIC EXTENDS INTO 2021:

Defenders and security professionals must remain vigilant to protect the critical infrastructure that connects and enables the modern world.

SPRG_008_EN-2104