Mexico

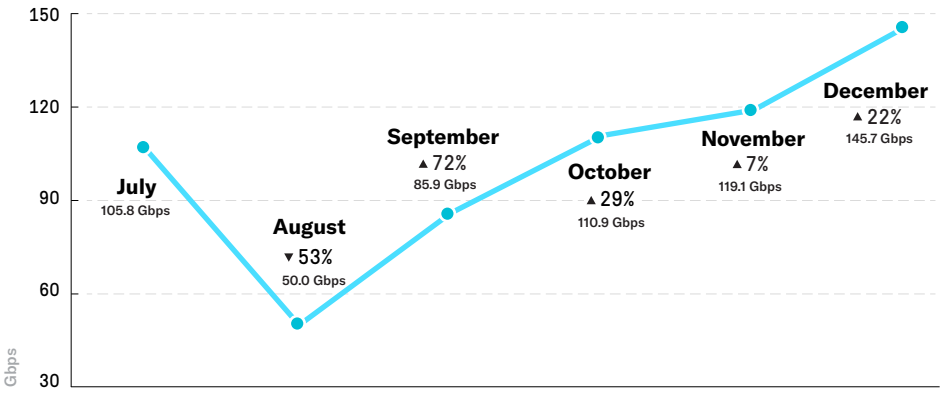
Key Metrics from the 2H 2020 NETSCOUT Threat Intelligence Report

As the COVID-19 pandemic triggered a massive shift in internet usage, cybercriminals quickly pounced, launching more than 10 million DDoS attacks aimed at crippling the very online services essential to remote work and online life. Vital pandemic industries such as ecommerce, streaming services, online learning, and healthcare all experienced increased attention from malicious actors, including those behind the Lazarus Bear Armada campaign of DDoS extortion attacks that hit thousands of companies worldwide. As the COVID-19 pandemic extends into 2021, we can logically expect to see threat actors targeting vulnerabilities exposed by the global crisis as well as discovering and using new attack vectors that poke at the weak spots of our new normal.

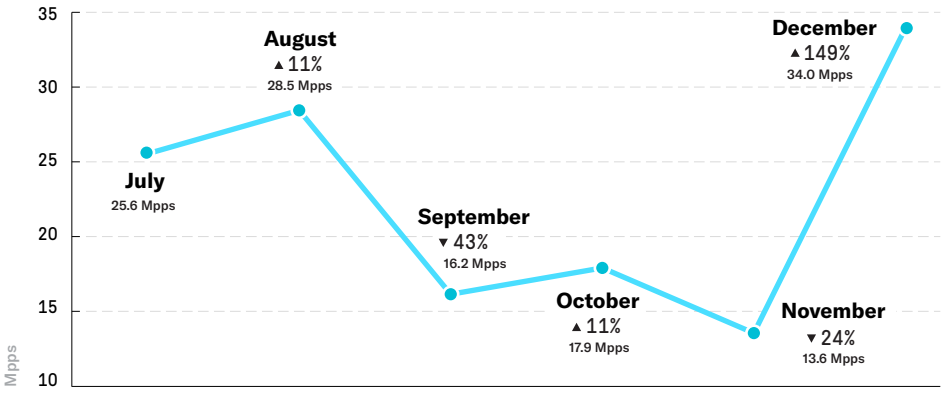
Impact Analysis

This was a record-breaking year for DDoS attacks—and that has to have an impact on global infrastructure, since DDoS attackers don't pay for transit costs. Instead, that cost is generally passed down to everyone who uses the internet. So we continued to dig into the details of how much traffic on the global internet is due solely to DDoS attacks by calculating the DDoS Attack Coefficient (DAC). This measurement illustrates the continual presence of DDoS traffic across all regions. In essence, it shows the "DDoS tax" that we all end up paying.

BANDWIDTH IMPACT PERCENTAGE CHANGE



THROUGHPUT IMPACT PERCENTAGE CHANGE



DDoS Statistics

Attack frequency	▲ 122%
Max throughput	▲ 30%
Average duration	▼ 10%
Max attack size	▼ 35%

Largest Attack

Size	103 GBPS
Speed	27.7 MPPS
Duration	41 MIN

Attack types

NTP Amplification, TCP ACK, DNS Amplification, ICMP, TCP SYN/ACK Amplification, TCP RST

Vector Attacks

Max number of vectors seen in a single attack **18**

TOP 5 VECTOR	# OF ATTACKS
DNS Amplification	30,988
CLDAP Amplification	17,020
ICMP	13,596
TCP SYN	13,521
TCP RST	7,581

NETSCOUT

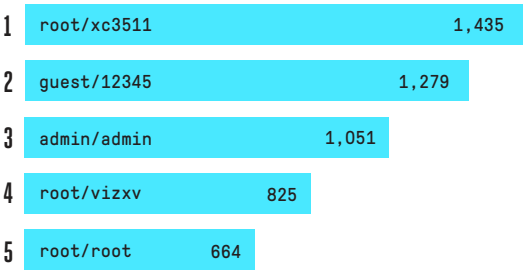
Top Ten Vertical Industries Under Attack

The following industry chart shows the most targeted sectors in 2020 by number of attacks.

RANK	VERTICAL	FREQUENCY	MAX ATTACK	MAX IMPACT	AVERAGE DURATION
1	Wired Telecommunications Carriers	41,566	101.2 Gbps	25.2 Mpps	20.5 Minutes
2	Data Processing, Hosting + Related Services	1,279	16.5 Gbps	3.2 Mpps	39.6 Minutes
3	Other Telecommunications	836	17.6 Gbps	6.8 Mpps	45.4 Minutes
4	Telecommunications Resellers	426	0.9 Gbps	0.2 Mpps	43.7 Minutes
5	Software Publishers	143	0.5 Gbps	0.1 Mpps	30.1 Minutes
6	Commercial Banking	128	0.3 Gbps	0.02 Mpps	29.6 Minutes
7	Research + Development in Biotechnology	110	1.1 Gbps	0.2 Mpps	32.8 Minutes
8	Internet Publishing and Broadcasting + Web Search Portals	86	1.1 Gbps	0.1 Mpps	38.9 Minutes
9	Computer Training	69	1.7 Gbps	0.2 Mpps	33.1 Minutes
10	Gypsum Product Manufacturing	64	0.1 Gbps	0.1 Mpps	35.4 Minutes

IoT

TOP FIVE USERNAME + PASSWORD COMBINATIONS



TOP FIVE EXPLOITS

EXPLOIT NAME	EDB-ID
/ctrlt/DeviceUpgrade_1 Huawei Router	45991
/setup.cgi Netgear Remote Code Execution	43055
/picsdesc.xml Realtex SDK — Miniigd UPnP SOAP	37169
/ws/v1/cluster/apps Hadoop YARN ResourceManager	45025
/GponForm/diag_Form Dasan GPON home routers	-----

The Big Picture

Explore the full 2H 2020 NETSCOUT Threat Intelligence Report to find the latest research into trends and activities across the global DDoS threat landscape.

READ THE REPORT

NETSCOUT

© 2021 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, and the NETSCOUT logo are registered trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. All other brands and product names and registered and unregistered trademarks are the sole property of their respective owners.

SECR_020_EN-2101