Brazil

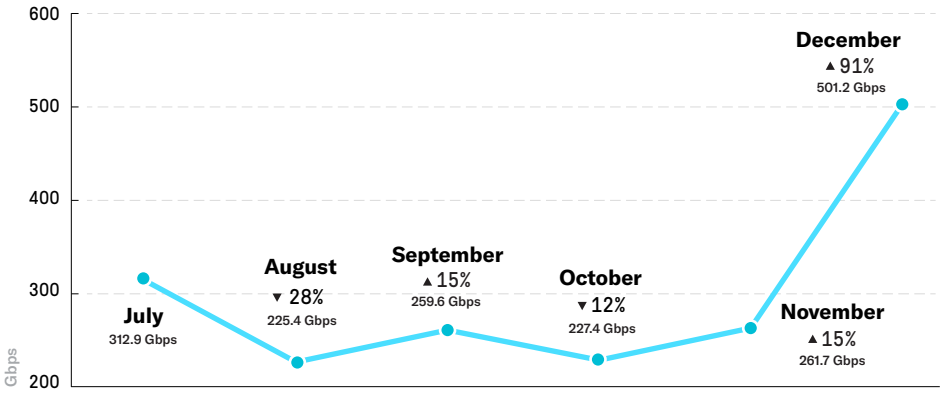
Key Metrics from the 2H 2020 NETSCOUT Threat Intelligence Report

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.

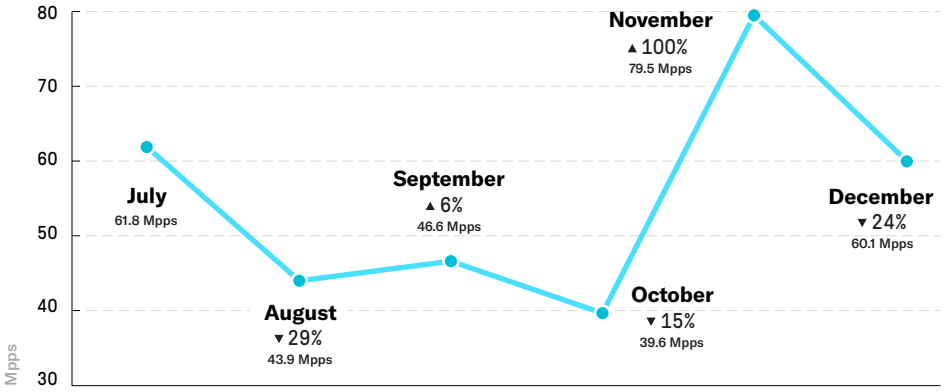
Impact Analysis

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	▲ 36%
Max throughput	▲ 68%
Average duration	▼ 48%
Max attack size	▼ 67%

Largest Attack

Size	313.5 GBPS
Speed	29.6 MPPS
Duration	192 MIN

Attack types

ICMP, DNS Amplification, Chargen Amplification, DNS, WS-DD Amplification

Vector Attacks

Max number of vectors seen in a single attack **22**

TOP 5 VECTOR	# OF ATTACKS
TCP ACK	130,897
DNS Amplification	78,972
TCP RST	70,554
TCP SYN	70,440
TCP SYN/ACK Amplification	62,636

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	Wireless Telecommunications Carriers	43,456	349.6 Gbps	29.9 Mpps	50.2 Minutes
2	Wired Telecommunications Carriers	5,052	134.5 Gbps	11.3 Mpps	91.4 Minutes
3	Electronic Computer Manufacturing	4,323	43.2 Gbps	6.8 Mpps	52.9 Minutes
4	Electronic Shopping + Mail-Order Houses	4,138	8.2 Gbps	2.0 Mpps	79.1 Minutes
5	Data Processing, Hosting + Related Services	3,413	49.5 Gbps	8.1 Mpps	70.2 Minutes
6	Other Telecommunications	3,143	84.0 Gbps	7.1 Mpps	91.7 Minutes
7	Internet Publishing, Broadcasting + Web Search Portals	1,976	104.2 Gbps	8.9 Mpps	56.1 Minutes
8	Religious Organizations	1,122	19.9 Gbps	19.6 Mpps	49.0 Minutes
9	Commerical Banking	812	5.5 Gbps	1.1 Mpps	71.5 Minutes
10	Telecommunications Resellers	721	12.8 Gbps	2.6 Mpps	31.7 Minutes

IoT

TOP FIVE USERNAME + PASSWORD COMBINATIONS

1	guest/12345	10,734
2	root/xc3511	9,697
3	admin/admin	7,393
4	root/vizxv	6,840
5	root/root	5,333

TOP FIVE EXPLOITS

EXPLOIT NAME	EDB-ID
/ctrlt/DeviceUpgrade_1 Huawei Router	45991
/picsdesc.xml Realtex SDK — Miniigd UPnP SOAP	37169
/setup.cgi Netgear Remote Code Execution	43055
/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_016_EN-2001