



Australia

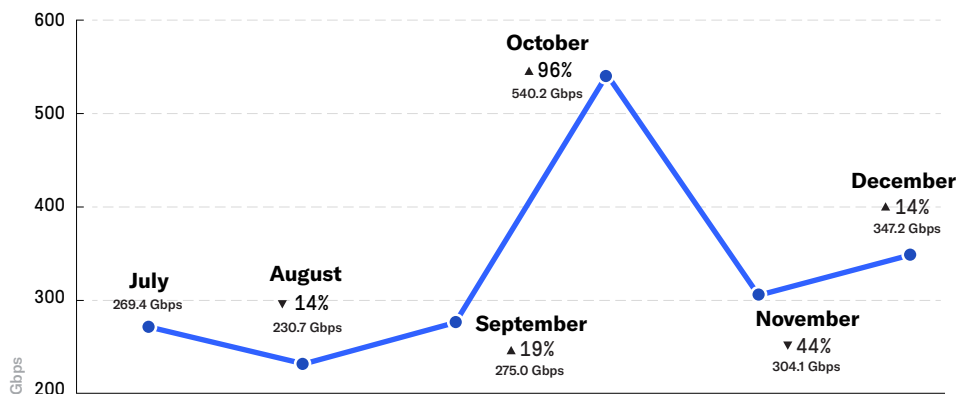
Key Metrics from the 2H 2020 NETSCOUT Threat Intelligence Report

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.

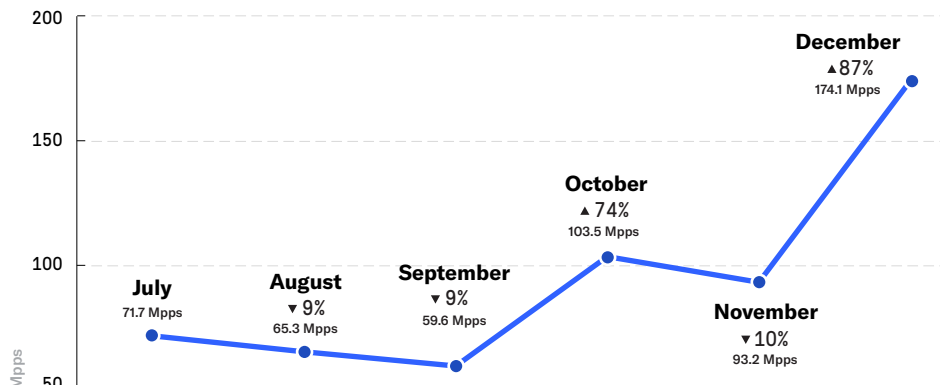
Impact Analysis

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	▲ 54%
Max throughput	▼ 3%
Average duration	▲ 27%
Max attack size	▲ 12%

Largest Attack

Size	223 GBPS
Speed	21.2 MPPS
Duration	10 MIN
Attack types	DNS Amplification, DNS, ICMP

Vector Attacks











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

TOP 5 VECTOR # OF ATTACKS

DNS Amplification	54,325
CLDAP Amplification	42,900
ICMP	41,529
TCP ACK	17,678
TCP SYN	11,717

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	6,667	380.2 Gbps	46.4 Mpps	54.3 Minutes
2	 Wireless Telecommunications Carriers	2,496	181.3 Gbps	22.5 Mpps	39.7 Minutes
3	 Data Processing, Hosting + Related Services	1,609	254.9 Gbps	33.6 Mpps	42.7 Minutes
4	 Electronic Computer Manufacturing	903	380.2 Gbps	46.4 Mpps	47.9 Minutes
5	 Electronic Shopping + Mail-Order Houses	691	380.2 Gbps	46.4 Mpps	42.8 Minutes
6	 Software Publishers	165	0.9 Gbps	0.1 Mpps	59.2 Minutes
7	 Internet Publishing, Broadcasting + Web Search Portals	161	0.9 Gbps	0.1 Mpps	33.1 Minutes
8	 Other Telecommunications	124	380.2 Gbps	46.4 Mpps	49.0 Minutes
9	 Landscaping Services	112	1.8 Gbps	0.2 Mpps	50.5 Minutes
10	 Other Services Related to Advertising	106	5.7 Gbps	0.7 Mpps	40.2 Minutes

IoT

TOP FIVE USERNAME + PASSWORD COMBINATIONS

1	root/xc3511	442
2	guest/12345	416
3	admin/admin	410
4	root/vizxv	365
5	root/root	277

TOP 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

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](#)