United Kingdom

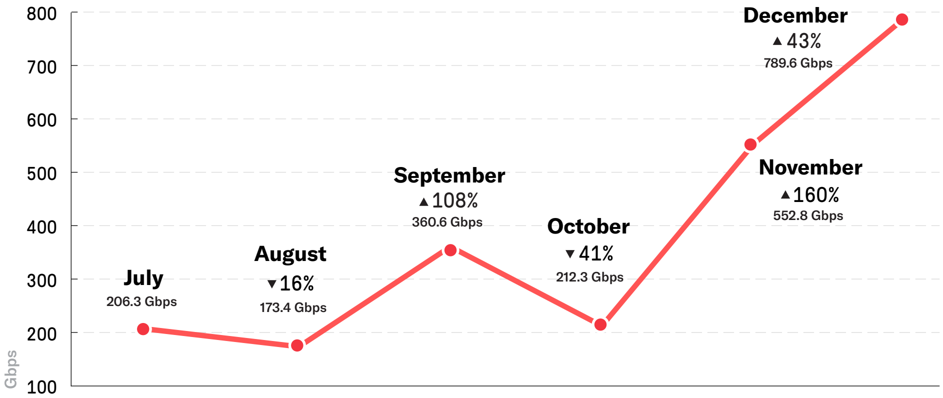
Key Metrics from the 2H 2020 NETSCOUT Threat Intelligence Report

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.

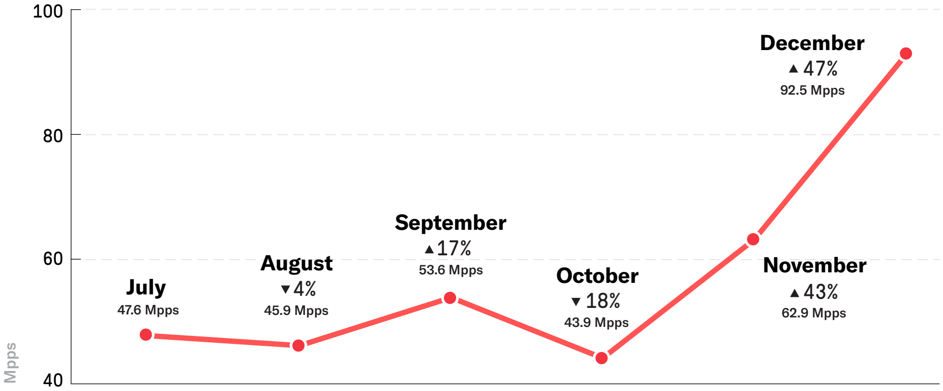
Impact Analysis

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	▲ 48%
Max throughput	▼ 60%
Average duration	▼ 27%
Max attack size	▼ 25%

Largest Attack

Size	185 GBPS
Speed	16.6 MPPS
Duration	123 MIN

Attack types

UDP, L2TP Amplification, ICMP, DNS, DNS Amplification, mDNS amplification, TCP ACK, TCP SYN, Memcached Amplification, TCP SYN/ACK Amplification, CLDAP Amplification, RIPv1 Amplification, NTP Amplification, MSSQLRS Amplification, SSDP Amplification, TCP RST, OpenVPN Amplification, Ubiquiti Amplification

Vector Attacks

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

TOP 5 VECTOR	# OF ATTACKS
DNS Amplification	129,987
ICMP	57,822
TCP SYN	57,146
CLDAP Amplification	56,750
TCP ACK	51,969

NETSCOUT

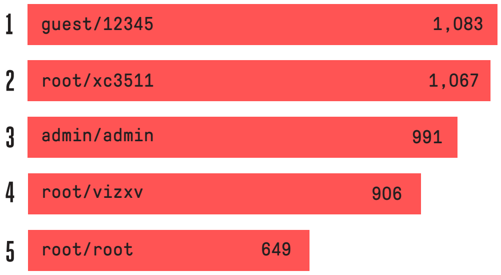
Top Ten Vertical Industries Under Attack

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**	21,076	72.4 Gbps	18.7 Mpps	41.2 Minutes
2	**Data Processing, Hosting + Related Services**	19,959	72.4 Gbps	18.7 Mpps	50.2 Minutes
3	**Wireless Telecommunications Carriers**	12,439	72.4 Gbps	15.3 Mpps	39.2 Minutes
4	**Electronic Computer Manufacturing**	8,190	66.5 Gbps	14.1 Mpps	60.8 Minutes
5	**Other Telecommunications**	7,136	72.4 Gbps	14.9 Mpps	69.9 Minutes
6	**Electronic Shopping + Mail-Order Houses**	6,808	66.5 Gbps	14.1 Mpps	58.5 Minutes
7	**Industrial Machinery + Equipment Merchant Wholesalers**	2,175	47.3 Gbps	3.9 Mpps	36.8 Minutes
8	**Support Services**	1,400	4.3 Gbps	1.1 Mpps	42.3 Minutes
9	**Internet Publishing, Broadcasting + Web Search Portals**	900	17.6 Gbps	5.4 Mpps	41.1 Minutes
10	**Offices of Dentists**	590	26.6 Gbps	2.9 Mpps	43.1 Minutes

IoT

TOP FIVE USERNAME + PASSWORD COMBINATIONS



TOP FIVE EXPLOITS

EXPLOIT NAME	EDB-ID
/ctrlt/DeviceUpgrade_1 Huawei Router	45991
/ws/v1/cluster/apps Hadoop YARN ResourceManager	45025
/picsdesc.xml Realtek SDK Miniigd UPnP SOAP	37169
/setup.cgi Netgear Remote Code Execution	43055
/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

SECR_032_EN-2101