



## KEY METRICS FROM THE 1H 2021 NETSCOUT THREAT INTELLIGENCE REPORT

# UNITED STATES



The massive shift to online life triggered by the COVID-19 pandemic prompted record-breaking levels of innovation by threat actors, and NETSCOUT's ATLAS Security Engineering and Response Team (ASERT) expects this long tail of attacker innovation to last well into 2021.

Bad actors launched approximately 5.4 million DDoS attacks in 1H 2021—yet another record-breaking number. In particular, attackers launched unprecedented numbers of DDoS attacks in the first quarter, boosting attack frequency by 20 percent over the same time period in 2020. Meanwhile, adversaries discovered or weaponized seven UDP reflection/amplification DDoS attack vectors and developed adaptive multivector attacks specifically tailored to exploit vulnerabilities of their targets. Vital components of the connectivity supply chain came under increased attack, while ransomware gangs added triple-extortion DDoS tactics to their repertoire and the Fancy Lazarus threat actor launched a new DDoS extortion campaign.

### Max Multivector Attack

Max number of vectors seen in a single attack

# 24

#### ATTACK VECTORS USED

1. Citrix-ICA amplification
2. CLDAP amplification
3. COAP amplification
4. DNS amplification
5. ICMP
6. IMPI amplification
7. ISAKMP
8. mDNS amplification
9. Memcached amplification
10. MSSQLRS amplification
11. NetBIOS amplification
12. NTP amplification
13. OpenVPN amplification
14. Plex amplification
15. RIPv1 amplification
16. rpcbnd amplification
17. SNMP amplification
18. SSDP amplification
19. STUN amplification
20. TCP ACK
21. TCP RST
22. TCP SYN
23. TCP SYN/ACK amplification
24. WS-DD amplification

### Top 5 Attack Vectors

<b>Dn</b> DNS amp	<b>Im</b> ICMP	<b>Ts</b> TCP SYN	<b>Ta</b> TCP ACK	<b>Tr</b> TCP RST
NUMBER OF ATTACKS 357,583	NUMBER OF ATTACKS 268,074	NUMBER OF ATTACKS 260,169	NUMBER OF ATTACKS 252,499	NUMBER OF ATTACKS 172,814

### DDoS Statistics

Attack Frequency	+7%
Max Throughput	-36%
Average Duration	+17%
Max Attack Size	+47%

### Largest Attack

Size	629.46 Gbps
Speed	55.24 Mpps
Duration	10,182 Seconds

### Max Peak Throughput

Date	01/01/2021
Max Throughput	359 Mpps

### Max Peak Bandwidth

Date	06/01/2021
Max Bandwidth	1.635 Tbps



## Top Ten Vertical Industries Under Attack

The following chart shows a sampling of the most targeted sectors in 1H 2021 by number of attacks.

RANK	VERTICAL	FREQUENCY	MAX ATTACK	MAX IMPACT	AVERAGE DURATION
1	 <b>Wired Telecommunications Carriers</b>	167,741	384.93 Gbps	50.72 Mpps	31.3 Minutes
2	 <b>Data Processing, Hosting + Related Services</b>	88,508	114.42 Gbps	48.84 Mpps	83.8 Minutes
3	 <b>Internet Publishing, Broadcasting + Web Search Portals</b>	66,947	198.69 Gbps	48.74 Mpps	101.8 Minutes
4	 <b>Electronic Computer Manufacturing</b>	34,200	100.29 Gbps	20.82 Mpps	63.1 Minutes
5	 <b>Electronic Shopping + Mail-Order Houses</b>	33,157	119.19 Gbps	57.85 Mpps	109.1 Minutes
6	 <b>Wireless Telecommunications Carriers (except Satellite)</b>	23,105	90.86 Gbps	19.71 Mpps	45.1 Minutes
7	 <b>All Other Telecommunications</b>	16,256	100.29 Gbps	19.59 Mpps	43.2 Minutes
8	 <b>Software Publishers</b>	8,574	112.28 Gbps	26.03 Mpps	86.9 Minutes
9	 <b>Colleges, Universities + Professional Schools</b>	6,046	32.56 Gbps	5.60 Mpps	47.6 Minutes
10	 <b>Computer Storage Device Manufacturing</b>	4,996	95.21 Gbps	20.82 Mpps	66.7 Minutes

## The Big Picture

Explore the full 1H 2021 NETSCOUT Threat Intelligence Report to find the latest research into trends and activities across the global DDoS threat landscape.

[VIEW THE INTERACTIVE 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\_015\_EN-2102 09/2021