



KEY METRICS FROM THE 1H 2021 NETSCOUT THREAT INTELLIGENCE REPORT

GERMANY

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

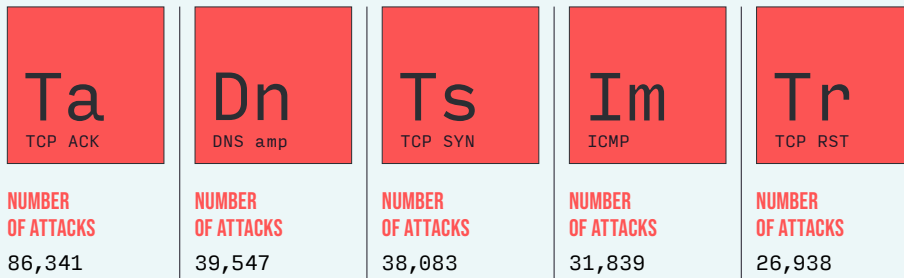
Max number of vectors seen in a single attack

31

ATTACK VECTORS USED

- | | | |
|-----------------------------|-----------------------------|-------------------------------|
| 1. Chargen amplification | 12. mDNS amplification | 23. STUN amplification |
| 2. Citrix-ICA amplification | 13. Memcached amplification | 24. TCP ACK |
| 3. CLDAP amplification | 14. MSSQLRS amplification | 25. TCP NULL |
| 4. COAP amplification | 15. NetBIOS amplification | 26. TCP RST |
| 5. DNS | 16. NTP amplification | 27. TCP SYN |
| 6. DNS amplification | 17. OpenVPN amplification | 28. TCP SYN/ACK amplification |
| 7. ICMP | 18. Plex amplification | 29. Ubiquiti amplification |
| 8. IMPI amplification | 19. RIPv1 amplification | 30. VSE amplification |
| 9. IPv4 Protocol 0 | 20. rcpbind amplification | 31. WS-DD amplification |
| 10. ISAKMP | 21. SNMP amplification | |
| 11. L2TP amplification | 22. SSDP amplification | |

Top 5 Attack Vectors



DDoS Statistics

Attack Frequency	-4%
Max Throughput	+27%
Average Duration	-3%
Max Attack Size	-19%

Largest Attack

Size	471.97 Gbps
Speed	270.50 Mpps
Duration	6,982 Seconds

Max Peak Throughput

Date	02/01/2021
Max Throughput	285 Mpps

Max Peak Bandwidth

Date	06/01/2021
Max Bandwidth	1.265 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	 Data Processing, Hosting + Related Services	25,895	114.42 Gbps	27.86 Mpps	50.3 Minutes
2	 Electronic Shopping + Mail-Order Houses	15,736	114.42 Gbps	25.67 Mpps	32.1 Minutes
3	 Wired Telecommunications Carriers	6,468	114.42 Gbps	25.67 Mpps	57.4 Minutes
4	 All Other Telecommunications	3,306	114.42 Gbps	25.67 Mpps	68.9 Minutes
5	 Wireless Telecommunications Carriers (except Satellite)	2,917	112.28 Gbps	22.58 Mpps	47.8 Minutes
6	 Electronic Computer Manufacturing	1,680	74.58 Gbps	16.41 Mpps	99.5 Minutes
7	 Computer Storage Device Manufacturing	687	74.88 Gbps	15.88 Mpps	115.0 Minutes
8	 Internet Publishing, Broadcasting + Web Search Portals	622	81.86 Gbps	87.52 Mpps	98.5 Minutes
9	 Other Residential Care Facilities	618	19.28 Gbps	2.55 Mpps	18.8 Minutes
10	 Offices of Dentists	392	22.65 Gbps	6.64 Mpps	37.8 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_019_EN-2102 09/2021