Distributed Denial of Service (DDoS)

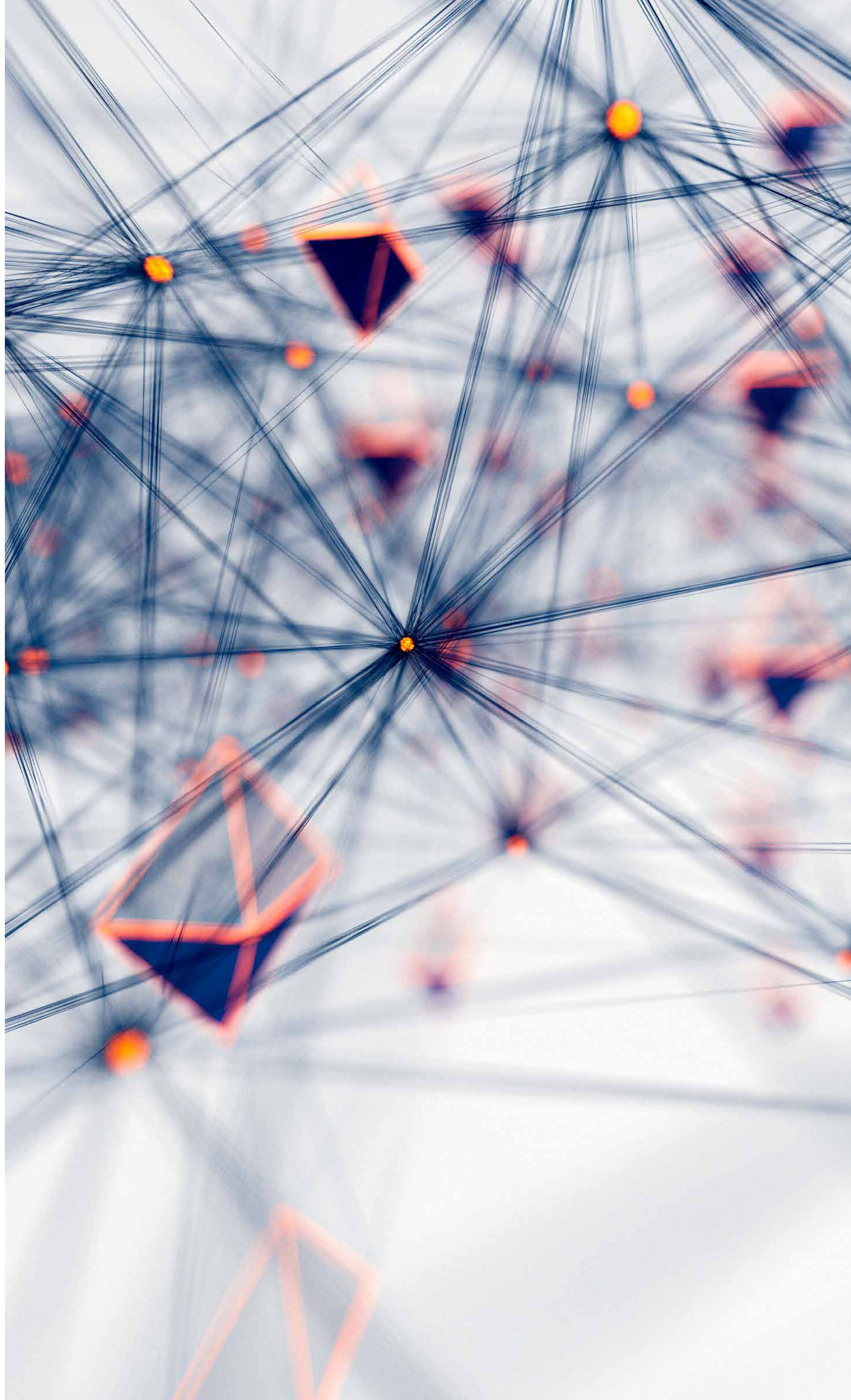
DDoS Statistical Report for 2021

NEXUSGUARD®

Table of Contents

Key Observations for 2021

- In 2021, the total attack count and average attack size both fell by 13.32% and 50.00% respectively compared to the figures registered in 2020.
- Compared to 2020, the maximum attack size increased by 296.62%, with the maximum attack size clocking in at 699.20 Gbps.
- UDP based attacks, while remaining the most predominant type of attack in 2021, decreased by 38.28% YoY. The number of TCP based, ICMP based and other attacks however, increased over the same period a year ago.
- Amplification attacks decreased YoY by 12.18% while Application attacks increased YoY by 54.94%.



Key Observations for 2021

Metrics

Total Attacks

vs. 2020

-13.32% ▼

Attack Sizes

Maximum

699.20 Gbps

vs. 2020

296.62% ▲

Average

0.76 Gbps

vs. 2020

-50.00% ▼

DDoS Attack Types

vs. 2020

UDP	DNS Amplification Attack	TCP ACK Attack	Application	Amplification	Bit and Piece
-20.86% ▼	-3.76% ▼	5.99% ▲	54.94% ▲	-12.18% ▼	-60.47% ▼

Key Observations for 2021

Trends

Over a 5 year period, there was a clear trend showing March consistently recording the highest number of attacks. Attacks in the summer months of June, July and August remained moderately active, but gradually began to tail off from September through to the end of the year. The cycle more or less repeated itself in the same vein the following spring, from March onwards.

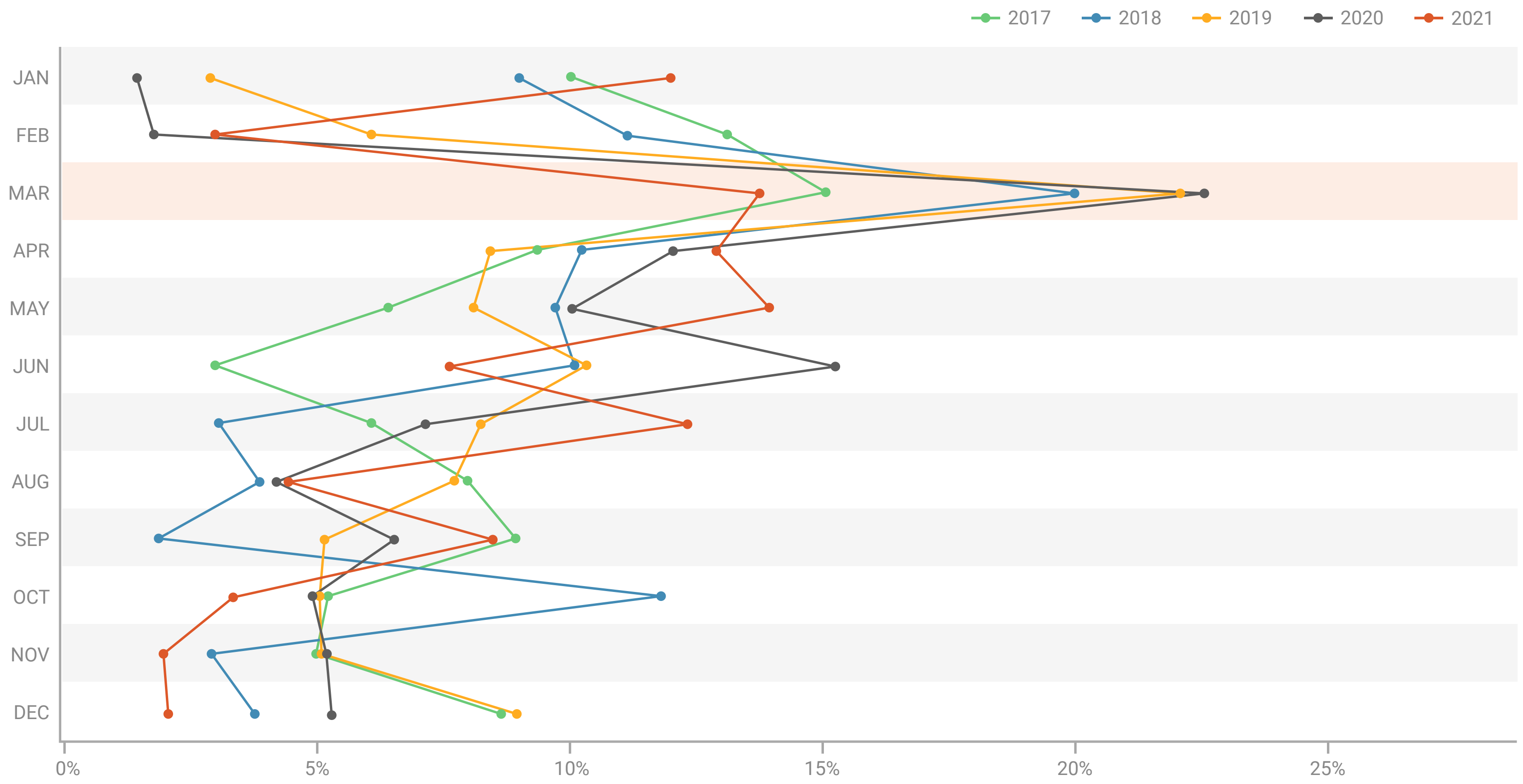


Figure 1 - DDoS Attack Trends from 2017 - 2021

2021 Attack Statistics

2021 Attack Statistics

Types of Attack Vectors

In 2021, UDP and DNS Amplification Attacks were the predominant two attack types, contributing 39.06% and 10.43% respectively, while TCP ACK Attacks ranked third at 9.70%. UDP and DNS Amplification Attacks decreased YoY by 20.86% and 3.76% respectively.

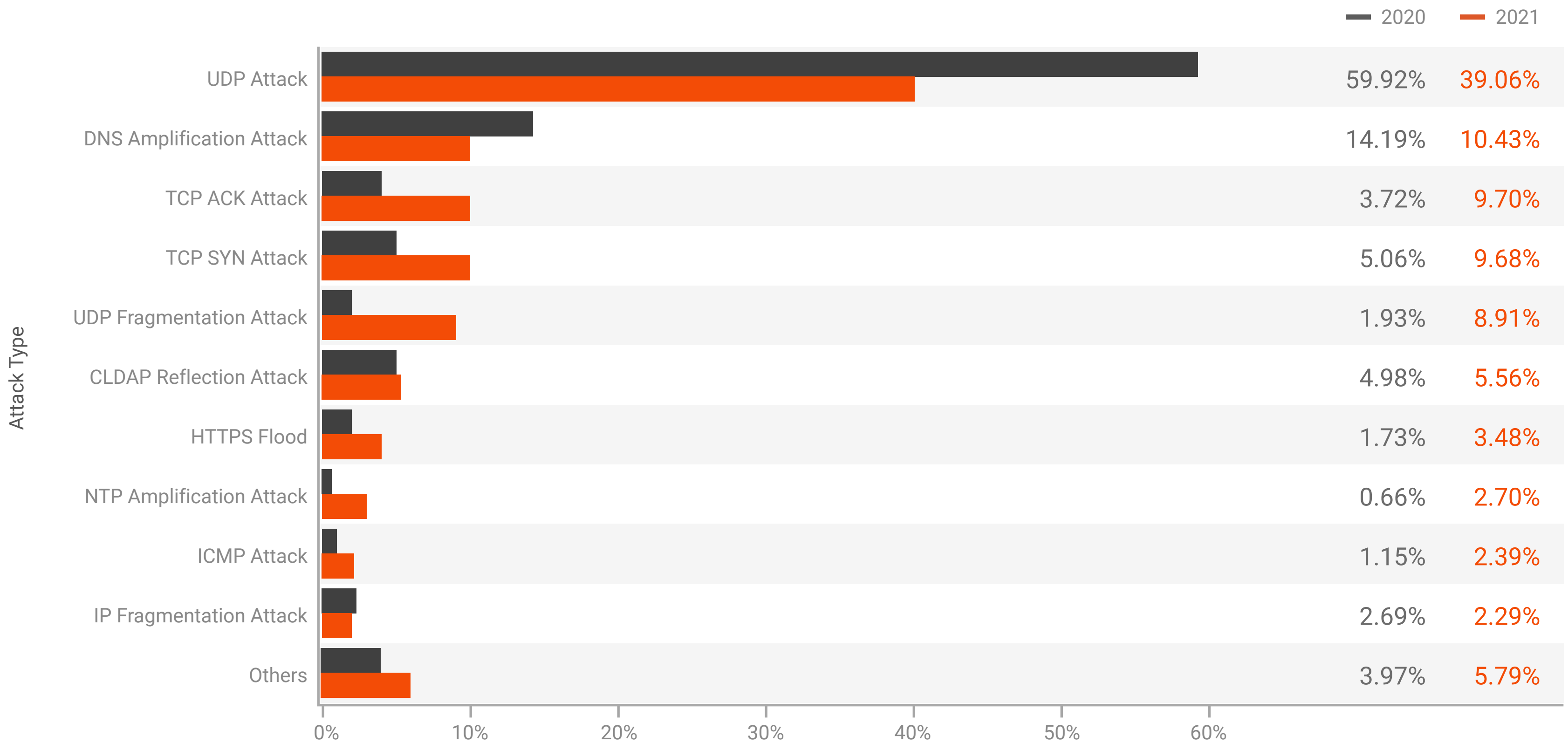


Figure 2 - Top 10 Attack Vectors in 2020 and 2021

2021 Attack Statistics

Top 3 Attack Vectors

1 UDP Attack

UDP (User Datagram Protocol) attacks can quickly overwhelm the defenses of unsuspecting targets. Speed in detection and response is key to thwarting attackers using this volumetric strategy. UDP frequently serves as a smokescreen to mask other malicious activities such as efforts to compromise personal identifiable information (PII) or the execution of malware or remote codes. When large numbers of UDP packets hit a targeted network, bandwidth is congested and a server's resources sapped, ultimately making them inaccessible.

2 DNS Amplification Attack

A DNS Amplification attack occurs when UDP packets with spoofed target IP addresses are sent to a publicly accessible DNS server. Each UDP packet makes a request to a DNS resolver, often sending an “ANY” request in order to receive a large number of responses. Attempting to respond, DNS resolvers send a large response to the target’s spoofed IP address. The target thus receives an enormous amount of responses from the surrounding network infrastructure, resulting in a DDoS attack. Because such a sizeable response can be created by a very small request, the attacker can leverage this tactic to amplify attacks with a maximum amplification factor of 54.

3 TCP ACK Attack

A TCP ACK attack occurs when a large quantity of ACK packets with spoofed IP addresses are sent to the victim server, forcing it to process each ACK packet it receives, rendering the server unreachable by legitimate requests. In more advanced TCP ACK attack techniques, the attacker will spoof the user’s source IP range to confuse the victim server running certain applications. Once any of these spoofed IP addresses matches a real source IP address, the connection between a real user and the application being run will be terminated as a result.

2021 Attack Statistics

Attacks by Category

Volumetric (Direct Flood) attacks, contributing 79.33% of the total attacks recorded in 2021, increased by 8.73% YoY, while Volumetric (Amplification) attacks, contributing 17.65%, decreased by 12.18% YoY. Application attacks represented 3.03% of the attacks in 2021, an increase of 54.94% YoY.

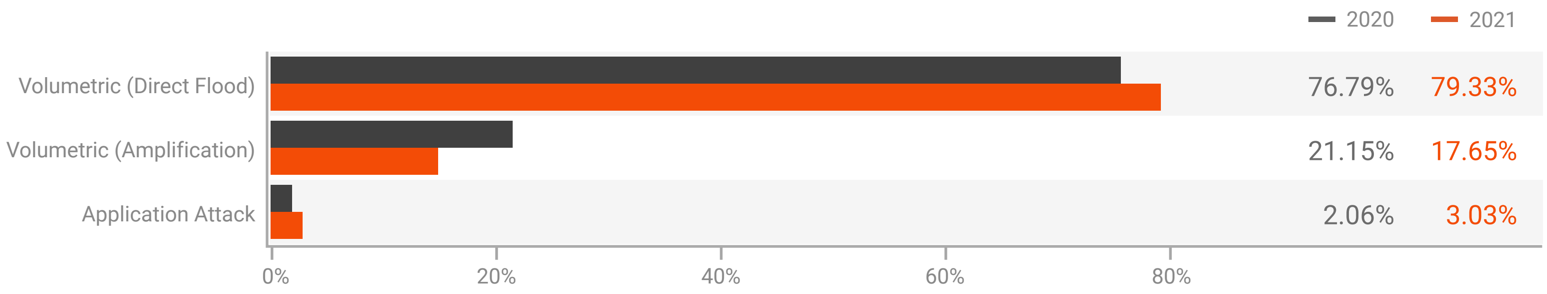


Figure 3 - Distribution of Attacks by Category in 2020 and 2021

Direct Flood attacks

9%

Amplification attacks

-12%

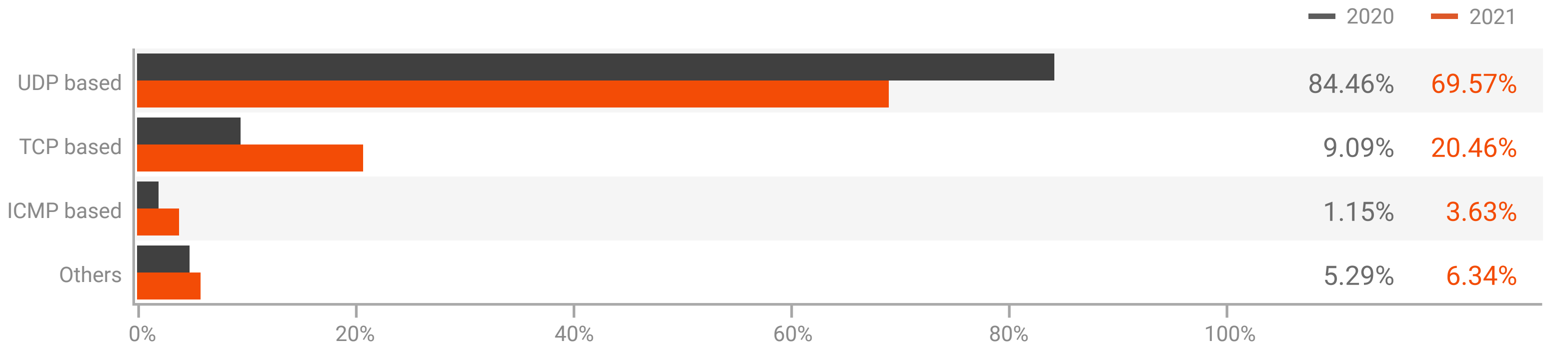
Application attacks

55%

2021 Attack Statistics

Attacks by Protocol

UDP and TCP based attacks were the predominant two attack types in 2021, contributing 69.57% and 20.46% respectively, while ICMP attacks ranked third at 3.63%. UDP based attacks decreased YoY by 38.28% and TCP based attacks increased YoY by 49.38%, while ICMP based attacks rose YoY by 63.47%.



	2020	2021
UDP based	84.46%	69.57%
TCP based	9.09%	20.46%
ICMP based	1.15%	3.63%
Others	5.29%	6.34%

Figure 4 - Distribution of Attacks by Protocol in 2020 and 2021

UDP based attacks

-38%

TCP based attacks

49%

ICMP based attacks

63%

2021 Attack Statistics

Quantity of Attack Vectors

Single-vector attacks played the leading role in 2021. 84.07% of attacks were single vector, while the rest were multi-vector.

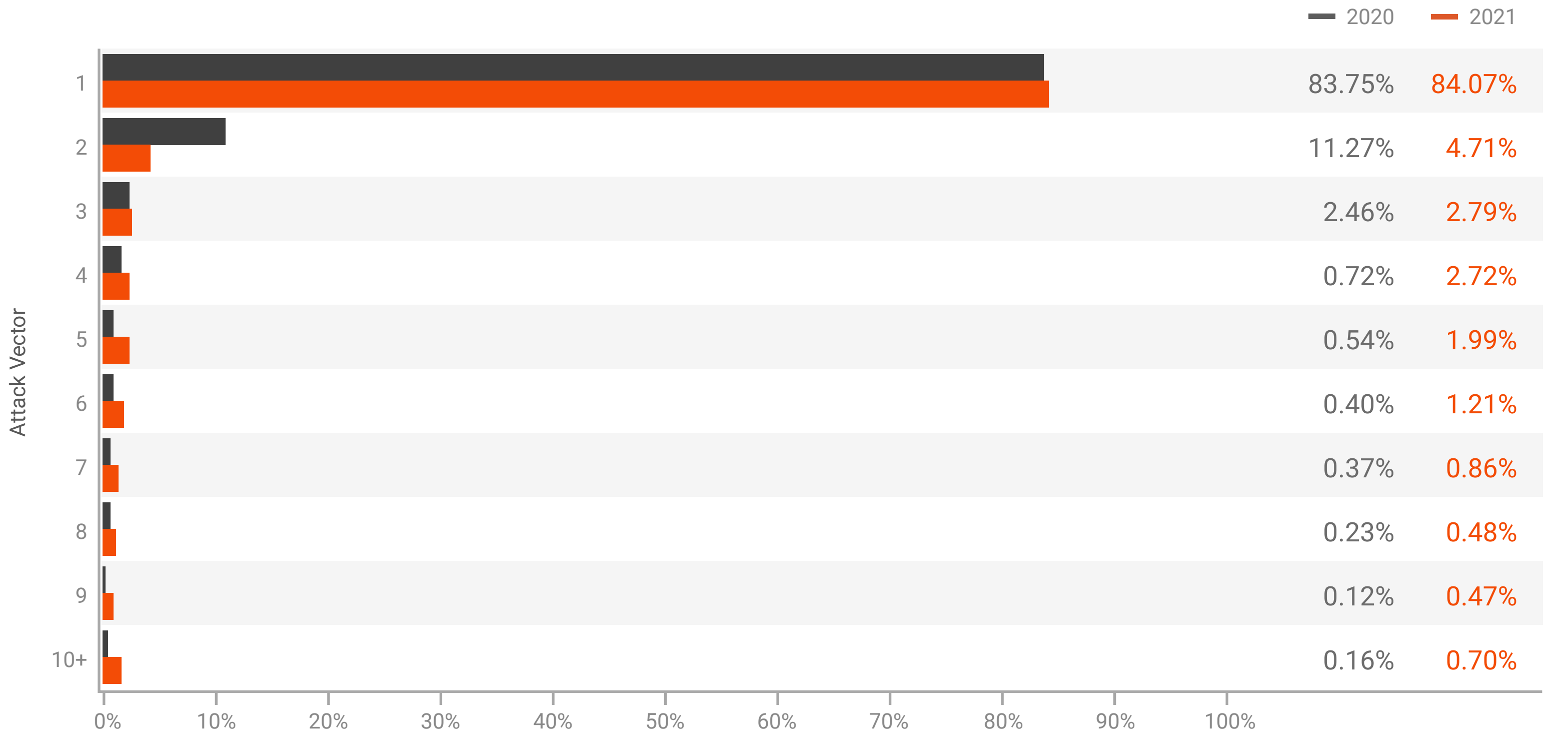


Figure 5 - Distribution of DDoS Attack Vectors in 2020 and 2021

Single-vector attacks

84%

Multi-vector attacks

16%

2021 Attack Statistics

Multi-Vector Attack Combinations

The most commonly used multi-vector attack combination recorded in 2021 was “CLDAP Reflection Attack coupled with UDP Fragmentation Attack”, contributing 6.82%. In second place was a combination of “CLDAP Reflection Attack, DNS Amplification Attack, ICMP Attack, TCP ACK Attack”, contributing 5.94%. And third place was composed of “CLDAP Reflection Attack, DNS Amplification Attack and ICMP Attack”, contributing 3.35%.

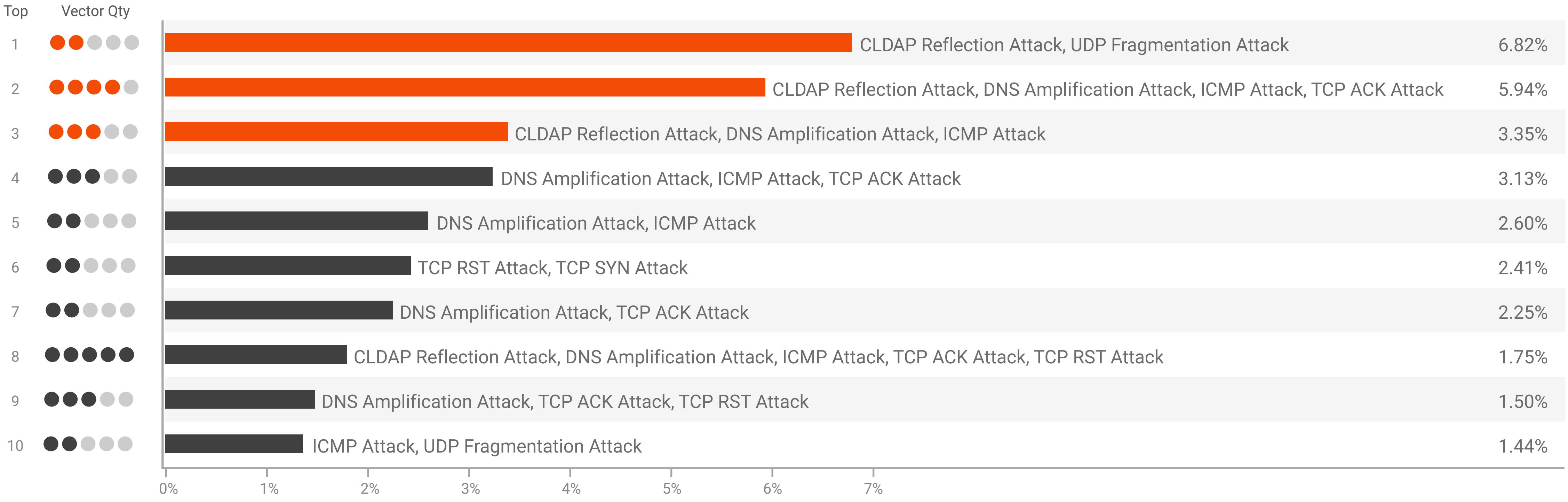


Figure 6 - Top 10 multi-vector combinations in 2021

2021 Attack Statistics

Attack Durations

Over 80% of attacks were shorter than 90 minutes, while the rest lasted longer than 90 minutes. 6.80% of attacks exceeded 1200 minutes. The average attack duration recorded in 2021 was 92.39 minutes, with the longest attack lasting 15,408.43 minutes. Both the maximum and average duration dropped by 75.83% and 48.66% respectively, YoY.

80%

of attacks were shorter than 90 minutes

Duration (Minutes)

	2020	2021
Maximum	63756.77	15408.43
Average	179.95	92.39

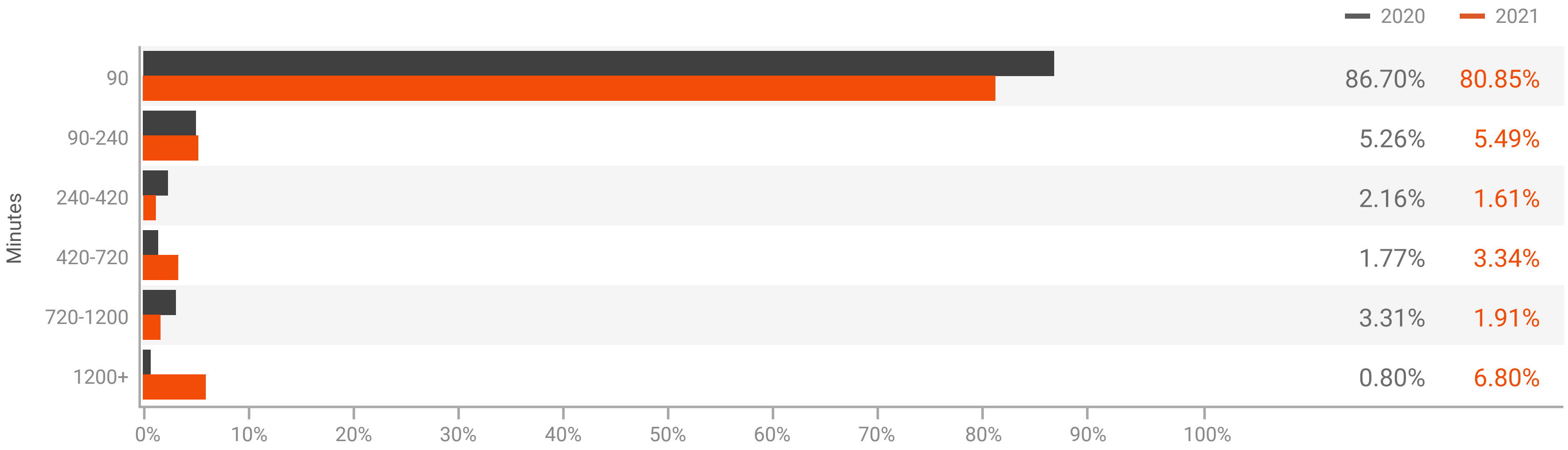


Figure 7 - Percentage Change of Attack Durations in 2020 and 2021

2021 Attack Statistics

Attack Size Distribution

Of the attacks recorded in 2021, 86.68% were smaller than 1Gbps. 7.88% ranged between 1Gbps - 10Gbps, and 5.44% were larger than 10Gbps.

86%

of attacks were smaller than 1Gbps

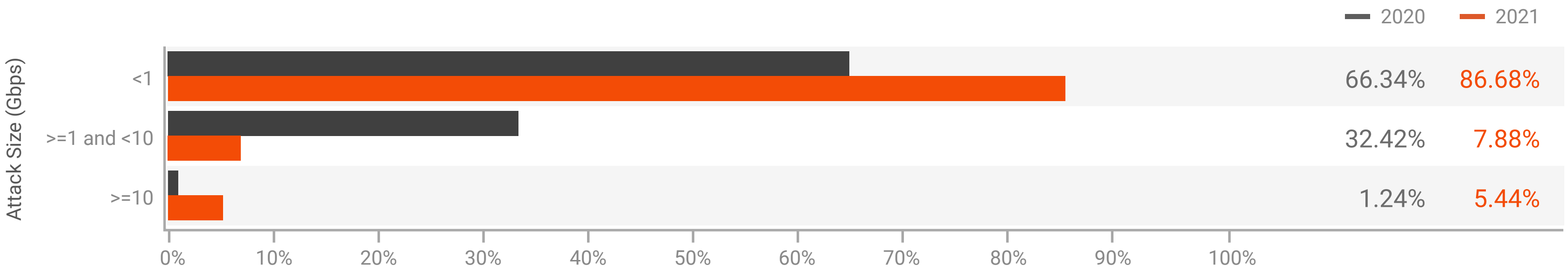


Figure 8 - Attack Size Distribution in 2020 and 2021

2021 Attack Statistics

Bit-and-Piece Attacks

ASN-level Communications Service Providers (CSPs) around the world, especially ISPs, continue to be impacted by the stealthy, sophisticated bit-and-piece attacks, which are carried out by drip-feeding doses of junk traffic into a large IP pool. Within each IP space, the junk traffic is small enough to bypass traditional threshold-based detection, but is big enough to clog the target when the bits and pieces are accumulated from different IPs.

Summary 1 - Bit-and-Piece Attacks in 2020 and 2021

		2020	2021	% increase
No. of Targeted ASN		301	119	-60.47%
No. Target Geolocations Country refer Sheet "Target Countries"		23	28	21.74%
Total IP prefixes under attack(Class C)		2,833	1,585	-44.05%
No. of targeted IP addresses per IP prefix	Minimum	10	10	0.00%
	Maximum	256	256	0.00%
Attack Count per IP	Minimum	40	40	0.00%
	Maximum	5,204,092	765,002	-85.30%
Attack Count per IP Prefix	Minimum	222	813	266.22%
	Maximum	5,219,918	1,821,606	-65.10%

Targeted ASNs

119

Total No. of IP Prefixes (Class C) Under Attack

1,585

Summary 2 - Bit-and-Piece Attack Types

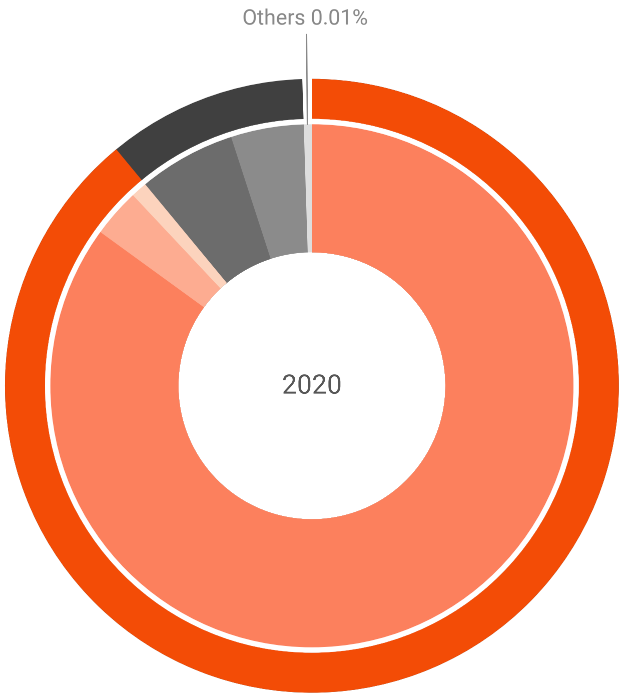
2020	2021
UDP Attack (44.22%)	TCP ACK Attack (35.45%)
DNS Amplification Attack (33.16%)	UDP Fragmentation Attack (15.07%)
CLDAP Reflection Attack (6.58%)	SSDP Amplification Attack (11.29%)
IP Fragmentation Attack (6.24%)	CLDAP Reflection Attack (10.74%)
SSDP Amplification Attack (2.49%)	UDP Attack (8.60%)
UDP Fragmentation Attack (1.60%)	CHARGEN Attack (7.81%)
TCP SYN Attack (1.56%)	DNS Amplification Attack (6.66%)
ICMP Attack (1.48%)	ICMP Attack (1.74%)
CHARGEN Attack (1.05%)	TCP SYN Attack (0.70%)
NTP Amplification Attack (0.68%)	IP Fragmentation Attack (0.40%)
DNS Attack (0.51%)	NTP Amplification Attack (0.35%)
MS SQL RS Amplification (0.13%)	IP BOGONS (0.35%)
TCP ACK Attack (0.13%)	TCP Null Attack (0.30%)
HTTPS Flood (0.08%)	HTTPS Flood (0.20%)
IP BOGONS (0.04%)	TCP RST Attack (0.20%)
SIP Flood (0.04%)	DNS Attack (0.10%)
	MDNS Amplification Attack (0.05%)

Summary 3 - Bit-and-Piece Targeted Geo-locations

2020	2021
Argentina, Australia, Bangladesh, Brazil, Canada, China, Greece, Hong Kong, Iran, Japan, Kuwait, Lebanon, Netherlands, Pakistan, Poland, Romania, Russian Federation, Singapore, South Africa, Taiwan, Turkey, Ukraine, United States,	Argentina, Austria, Bangladesh, Brazil, Bulgaria, Chile, China, Colombia, Czechia, France, Germany, Hong Kong, India, Indonesia, Israel, Norway, Pakistan, Philippines, Seychelles, Singapore, SouthAfrica, SriLanka, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Kingdom, United States

Source Distribution of Application Attacks[1]

MacOS devices contributed to 17.07% of all application attack traffic, while Windows-powered PCs and notebooks contributed 41.99%. Mobile iOS devices such as iPads and iPhones made up 3.37% of all application attack traffic, whereas android devices accounted for 14.32%



Source Distribution of Application Attacks

	2020	2021
🟥 **Computers and Servers**	**88.96%**	**81.92%**
🟥 Windows OS	85.39%	41.99%
🟥 Other OS	3.03%	22.86%
🟥 Macintosh OS	0.54%	17.07%
⬛ **Computers and Servers**	**11.04%**	**17.82%**
⬛ Windows OS	6.08%	3.37%
⬛ Other OS	4.96%	14.32%
⬛ Macintosh OS	0.00%	0.13%

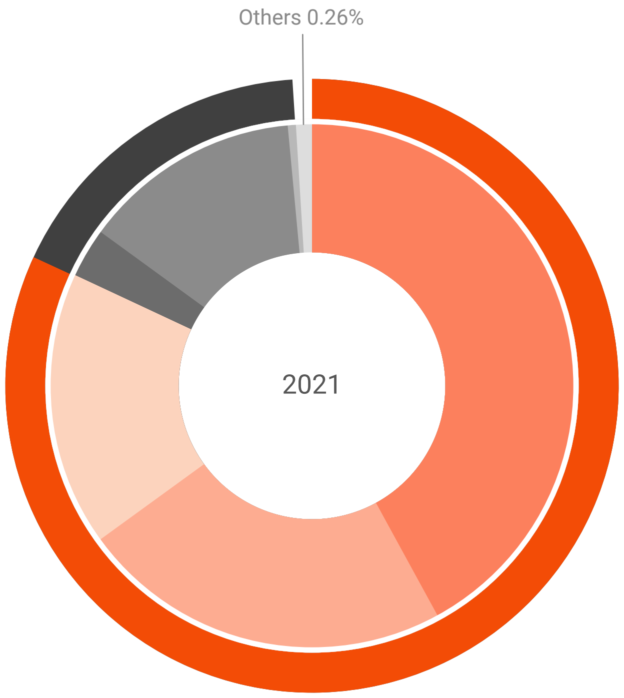


Figure 9 - Source Distribution of Application Attacks in 2020 and 2021

[1] Untraceable volumetric attacks transmitted with spoofed IP addresses such as TCP SYN, ICMP, and DNS were not included in our sampling. Only traceable attacks like HTTP/HTTPS Flood with real source IP addresses were counted. Attack traffic produced by mobile botnets are identified based on the following criteria: malicious traffic from mobile gateway IP addresses, attack patterns in user-agent, URL, HTTP header, etc. that are unique to mobile botnets.

2021 Attack Statistics

Application Attack Source Distribution (IP Reputation)

Top 10 Application Attack Source Distribution (IP Reputation) in Global 2021

	2021
Thailand	39.28%
China	16.15%
United States	12.23%
Turkey	7.44%
India	3.82%
Indonesia	2.64%
Singapore	2.52%
Hong Kong	1.94%
Australia	1.61%
Malaysia	1.51%
Others(231 Regions)	10.87%

Top 10 Application Attack Source Distribution (IP Reputation) in APAC 2021

	2021
Thailand	53.95%
China	22.18%
India	5.25%
Indonesia	3.62%
Singapore	3.46%
Hong Kong	2.66%
Australia	2.22%
Malaysia	2.08%
Philippines	1.29%
Japan	0.91%
Others(27 Regions)	2.38%

Application Attack Source by Autonomous System Number (ASN) – Global & Regional

Top 10 ASN Attacks Rankings in Global 2021

	AS Name	2021
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	8.85%
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	7.49%
AS24940	HETZNER-AS, DE	4.12%
AS15897	VODAFONETURKEY, TR	3.05%
AS37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN	2.71%
AS16135	TURKCELL-AS Turkcell A.S., TR	2.49%
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	2.25%
AS23693	TELKOMSEL-ASN-ID PT. Telekomunikasi Selular, ID	2.18%
AS33387	NOCIX, US	2.00%
AS4760	HKTIMS-AP HKT Limited, HK	1.91%

Top 10 ASN Attacks Rankings in APAC 2021

	AS Name	2021
AS4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	15.07%
AS4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	12.75%
AS37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN	4.61%
AS9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN	3.84%
AS23693	TELKOMSEL-ASN-ID PT. Telekomunikasi Selular, ID	3.71%
AS4760	HKTIMS-AP HKT Limited, HK	3.25%
AS45090	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	2.51%
AS9381	HKBNES-AS-AP HKBN Enterprise Solutions HK Limited, HK	2.33%
AS9269	HKBN-AS-AP Hong Kong Broadband Network Ltd., HK	2.25%
AS45102	CNNIC-ALIBABA-US-NET-AP Alibaba US Technology Co., Ltd., CN	2.00%

Top 10 ASN Attacks Rankings in EMEA 2021

	AS Name	2021
AS24940	HETZNER-AS, DE	15.87%
AS15897	VODAFONETURKEY, TR	11.75%
AS16135	TURKCELL-AS Turkcell A.S., TR	9.59%
AS20978	TT_MOBIL Istanbul, TR	6.98%
AS9121	TTNET, TR	6.78%
AS47331	TTNET, TR	4.81%
AS12978	DOGAN-ONLINE, TR	4.23%
AS34984	TELLCOM-AS, TR	4.01%
AS16276	OVH, FR	3.93%
AS47524	TURKSAT-AS, TR	2.70%

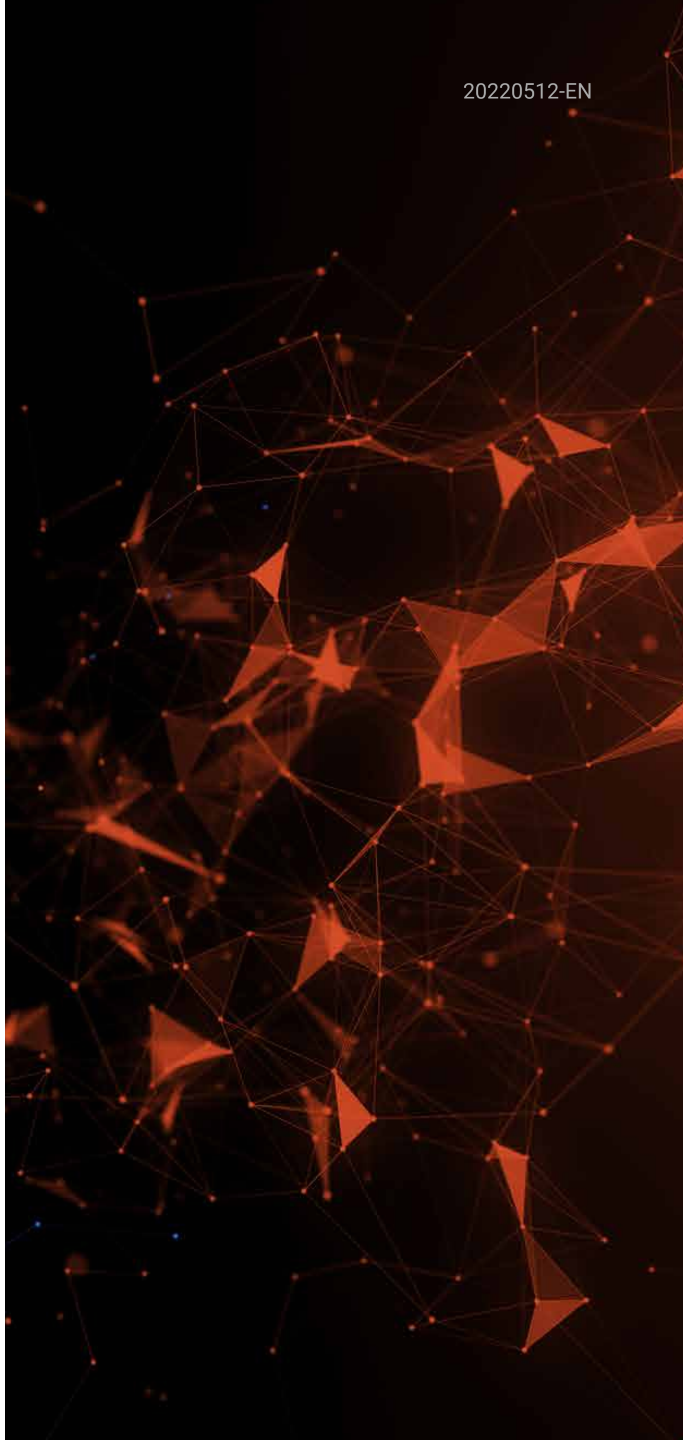
Top 10 ASN Attacks Rankings in Americas 2021

	AS Name	2021
AS33387	NOCIX, US	13.03%
AS18450	WEBNX, US	12.24%
AS16509	AMAZON-02, US	7.62%
AS7922	COMCAST-7922, US	3.86%
AS174	COGENT-174, US	3.65%
AS14061	DIGITALOCEAN-ASN, US	2.96%
AS15169	GOOGLE, US	2.74%
AS8075	MICROSOFT-CORP-MSN-AS-BLOCK, US	2.40%
AS7018	ATT-INTERNET4, US	2.26%
AS21928	T-MOBILE-AS21928, US	2.23%

Methodology

As a global leader in Distributed Denial of Service (DDoS) attack mitigation, Nexusguard observes and collects real-time data on threats facing enterprise and service-provider networks worldwide. Threat intelligence is gathered via attack data, research, publicly available information, Honeypots, ISPs, and logs recording traffic between attackers and their targets. The analysis conducted by our research team identifies vulnerabilities and measures attack trends worldwide to provide a comprehensive view of DDoS threats.

Attacks and hacking activities have a major impact on cybersecurity. Because of the comprehensive, global nature of our data sets and observations, Nexusguard is able to evaluate DDoS events in a manner that is not biased by any single set of customers or industries. Many zero-day threats are first seen on our global research network. These threats, among others, are summarized in the quarterly Statistical Report.



20220512-EN

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communication service providers to deliver DDoS protection solution as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

NEXUSGUARD®

www.nexusguard.com