Distributed Denial of Service (DDoS)

DDoS Statistical Report for 2022

NEXUSGUARD®

Table of Contents

Unveiling the Global Shift in DDoS Threat Landscape

Embedded within the 2022 DDoS Threat Report is a comprehensive research around the shift in the global threat landscape of DDoS. This annual report by Nexusguard studied increases in DDoS attacks between 2021 and 2022, including single-target network layer attacks and multi-thread application attacks.

Cyber attackers continue to alter their threat vectors by attacking application platforms, online database systems, and cloud-based storage. Attacking these critical infrastructures embedded within Internet Service Providers (ISPs) has a much more significant global effect as more organizations have moved their workloads to cloud providers.

DDoS attacks are standard cyber attacks on organizations, social engineering ransomware and supply chain attacks. These attacks target a system's crucial functions essential to day-to-day operations. Cyber attackers prefer DDoS attacks because they are efficient and have the necessary resources for a successful attack. Organizations typically run parts of their process on an internet site or internal database. In reviewing Nexusguard's annual statistical report in 2021 compared to 2022, threat actors turned their attention against mobiles and less against servers and PCs.

Key Observations for 2022

- In 2022, the total attack count and average attack size both increased by 115.07% and decreased 22.37% respectively compared to the figures registered in 2021.
- Compared to 2021, the maximum attack size decreased by 48.24%, with the maximum attack size clocking in at 361.9 Gbps.
- UDP based attacks remained the most predominant type of attack in 2022, increasing by 121.25% YoY. The number of TCP based attacks and other attacks also increased over the same period a year ago.
- Amplification attacks increased YoY by 414.63%, while Application attacks shot up by 718.08% YoY.

Key Observations for 2022

Metrics

Total Attacks

vs. 2021

115.07% ▲

Attack Sizes

Maximum

361.90 Gbps

vs. 2021

-48.24% ▼

Average

0.59 Gbps

vs. 2021

-22.37% ▼

Top 3 Attack Types

1

NTP Amplification Attack

vs. 2021

2,472.03% ▲

2

Memcached Attack

vs. 2021

28,233.16% ▲

3

UDP Attack

vs. 2021

72.71% ▲

DDoS Attack Category

Volumetric (Amplification)

vs. 2021

414.63% ▲

Volumetric (Direct Flood)

vs. 2021

-0.23% ▼

Application Attack

vs. 2021

718.08% ▲

Key Observations for 2022

Trends

Over a 5 year span, March recorded its lowest number of attacks, while September reached its highest ever attack count. The period between April and June saw the lowest number of attacks, with attacks decreasing further from October onwards, following the spike in September.

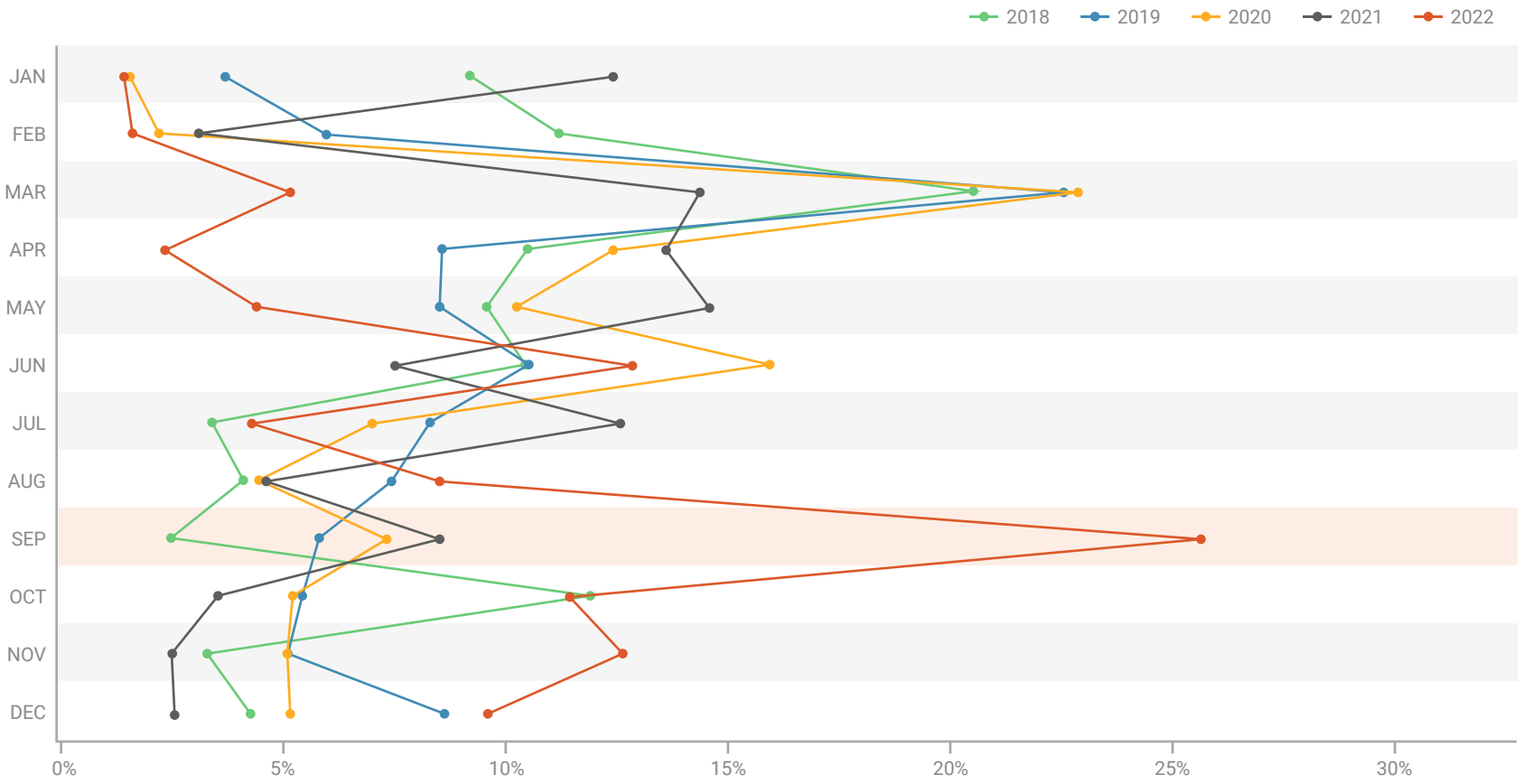
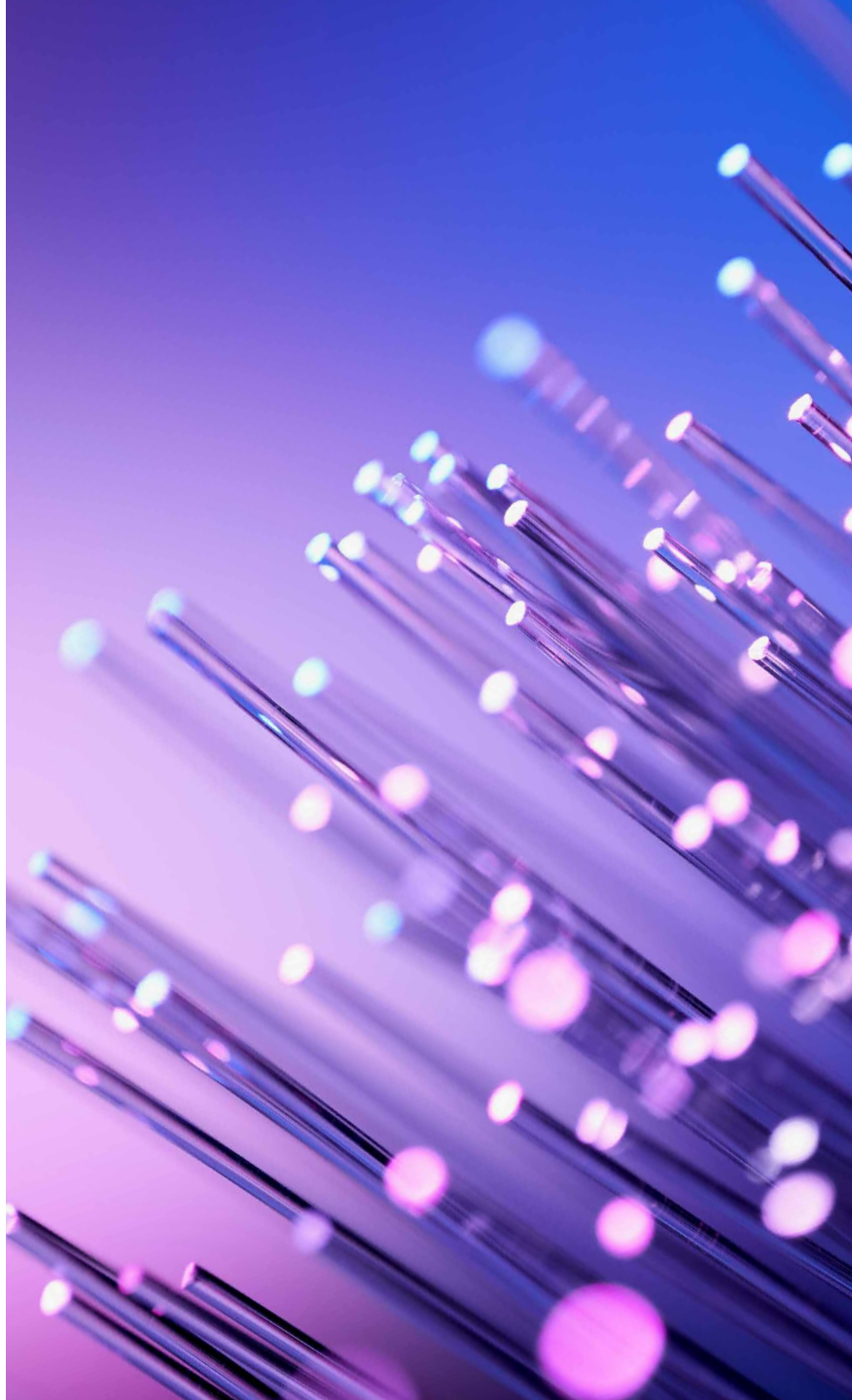


Figure 1 - DDoS Attack Trends from 2018 - 2022

2022 Attack Statistics

A DDoS attacker can exploit normal behavior between network devices and servers and target the networks connected through the Internet. A notable trend in the report shows that DDoS attacks continue to destroy the pipelines or devices providing the bandwidth as a primary attack destination



2022 Attack Statistics

Types of Attack Vectors

In 2022, NTP Amplification and Memcached Attacks were the predominant two attack types, contributing 31.01% and 14.33% respectively, while UDP Attacks ranked third at 13.21%. NTP Amplification and Memcached Attacks increased YoY by 2472.03% and 28233.16% respectively.

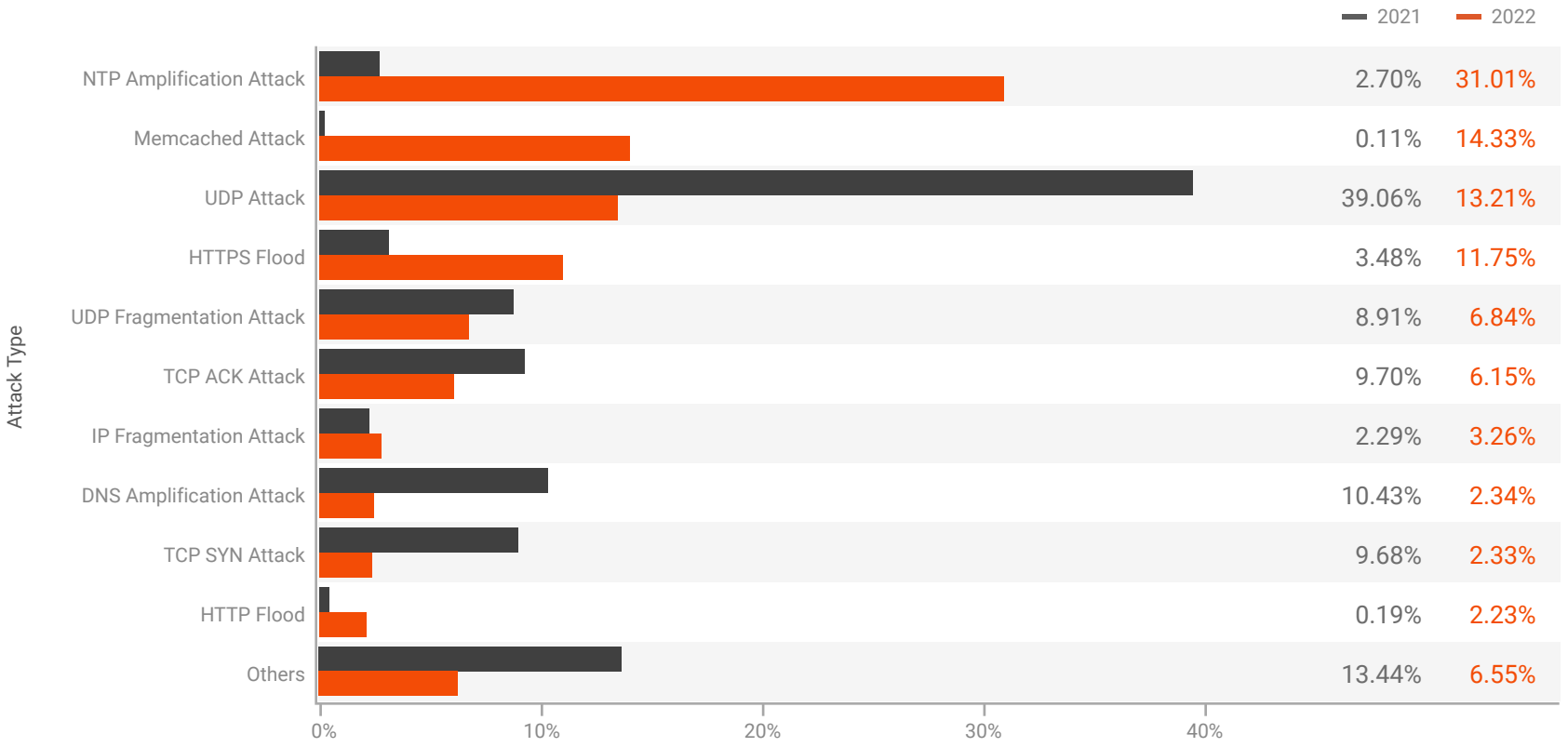


Figure 2 - Top 10 Attack Vectors in 2021 and 2022

2022 Attack Statistics

Top 3 Attack Vectors

1 NTP Amplification Attack

An NTP amplification attack is a Distributed Denial of Service (DDoS) attack in which an attacker spoofs a victim's IP address, and exploits an open Network Time Protocol (NTP) server to overwhelm the victim's network or server with amplified User Datagram Protocol (UDP) traffic.

According to US-Cert, the bandwidth amplification factor during such attacks can be as high as 556.9x.

2 Memcached Attacks

A Memcached Distributed Denial of Service (DDoS) attack is a cyber attack aimed at Memcached, a general-purpose distributed memory caching system used to speed up dynamic database-driven websites and applications.

The attacker spoofs requests to a compromised UDP memcached server that floods a targeted victim with traffic, potentially overloading the victim's resources.

According to US-Cert, the bandwidth amplification factor during such attacks can be as high as 51000x.

3 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.

2022 Attack Statistics

Attacks by Category

Volumetric (Amplification) attacks, contributing 51.28% of the total attacks recorded in 2022, increased by 414.63% YoY, while Volumetric (Direct Flood) attacks, contributing 34.37%, decreased by 0.23% YoY. Application attacks represented 13.97% of the attacks in 2022, an increase of 718.08% YoY.

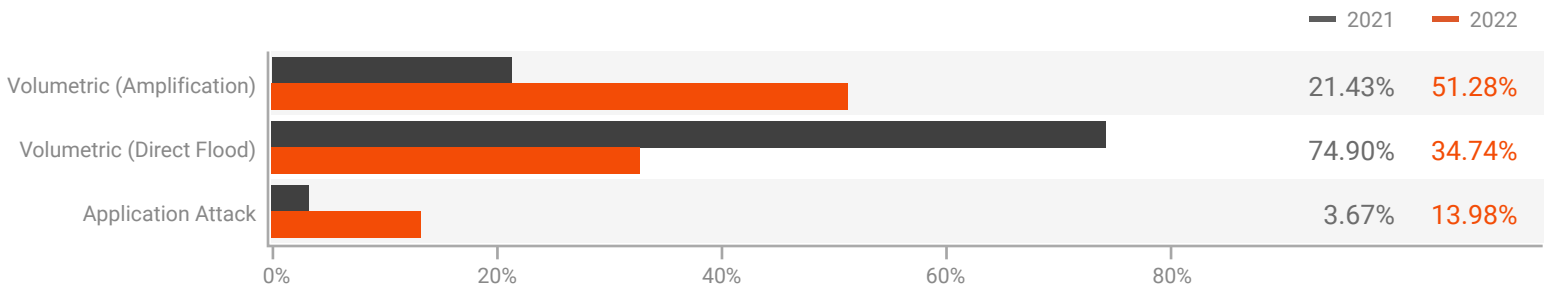


Figure 3 - Distribution of Attacks by Category in 2021 and 2022

Amplification attacks

+415%

Direct Flood attacks

-0.23%

Application attacks

+718%

2022 Attack Statistics

Attacks by Protocol

UDP and TCP based attacks were the predominant two attack types in 2022, contributing 72.49% and 23.00% respectively, while ICMP attacks ranked fourth at 0.64%. UDP based attacks increased YoY by 121.25% and TCP based attacks increased YoY by 102.71%, while ICMP based attacks decreased YoY by 42.15%.

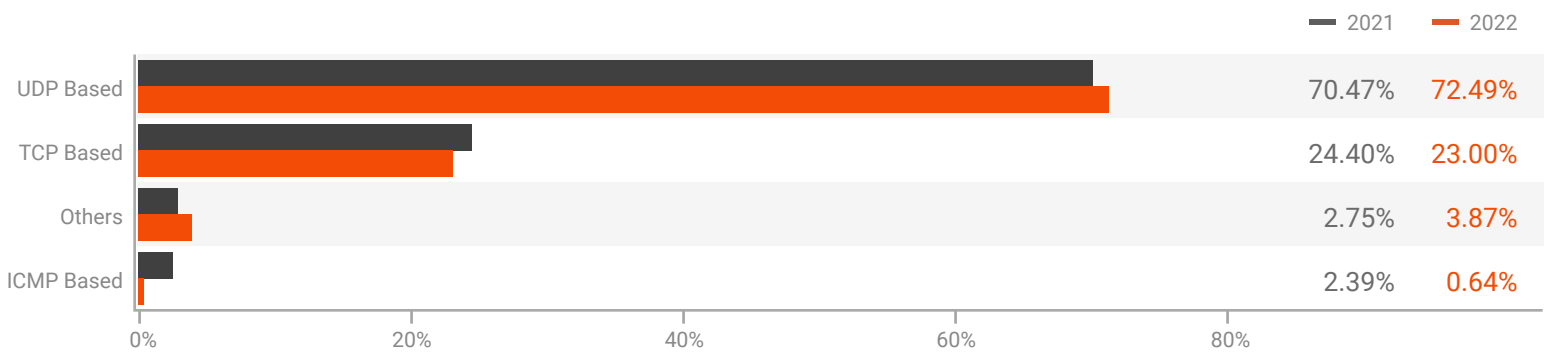


Figure 4 - Distribution of Attacks by Protocols in 2021 and 2022

UDP based attacks

+121%

TCP based attacks

+103%

2022 Attack Statistics

Quantity of Attack Vectors

Single-vector attacks played the leading role in 2022. 85.64% of attacks were single vector, while the rest were multi-vector.

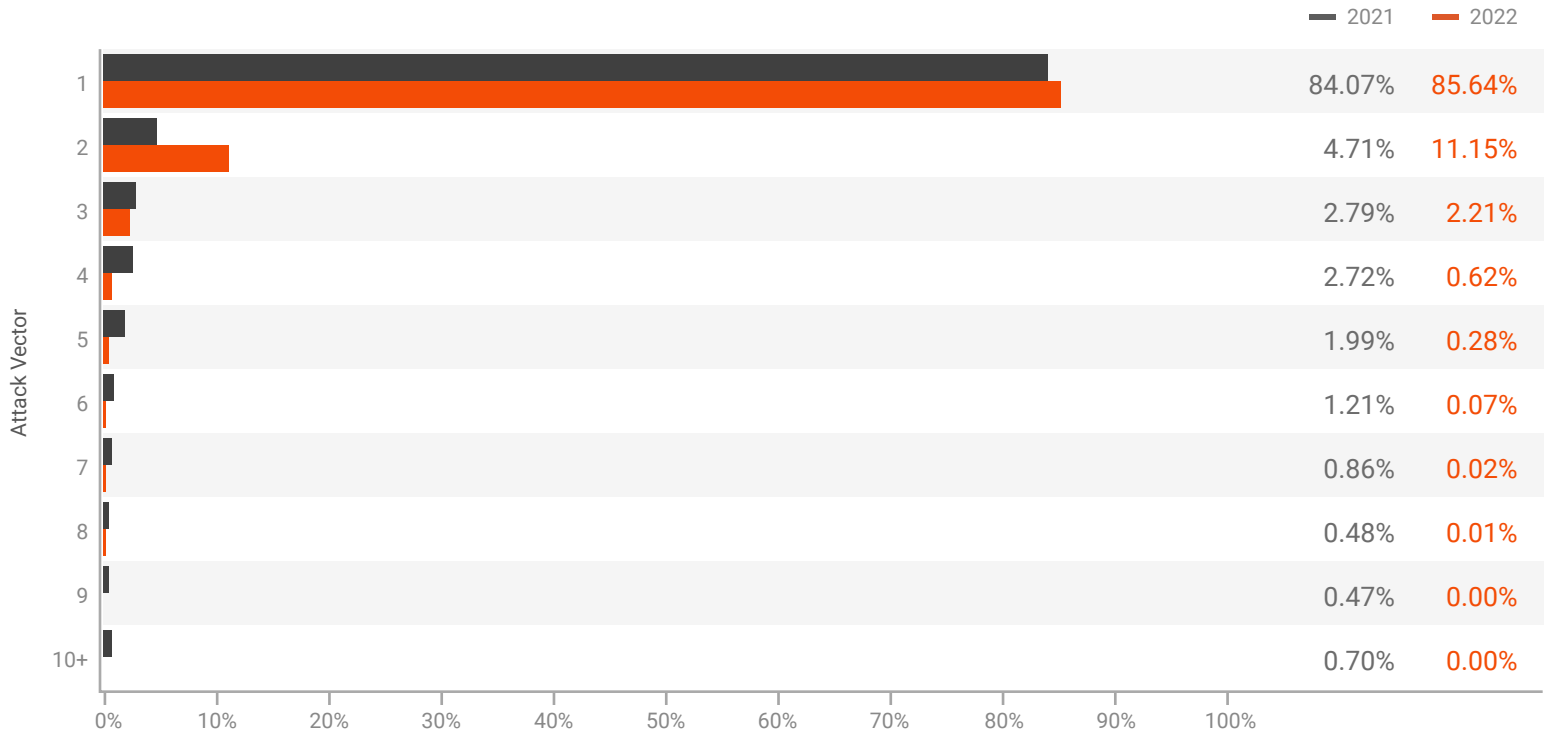


Figure 5 - Distribution of DDoS Attack Vectors in 2021 and 2022

Single-vector attacks

86%

Multi-vector attacks

14%

2022 Attack Statistics

Multi-Vector Attack Combinations

The most commonly used multi-vector attack combination recorded in 2022 was “TCP ACK Attack coupled with UDP Attack”, contributing 18.86%. In second place was a combination of “MEMCACHED Attack and NTP Amplification Attack”, contributing 12.02%. And third place was a combination of “HTTP Flood and HTTPS Flood”, contributing 6.78%.

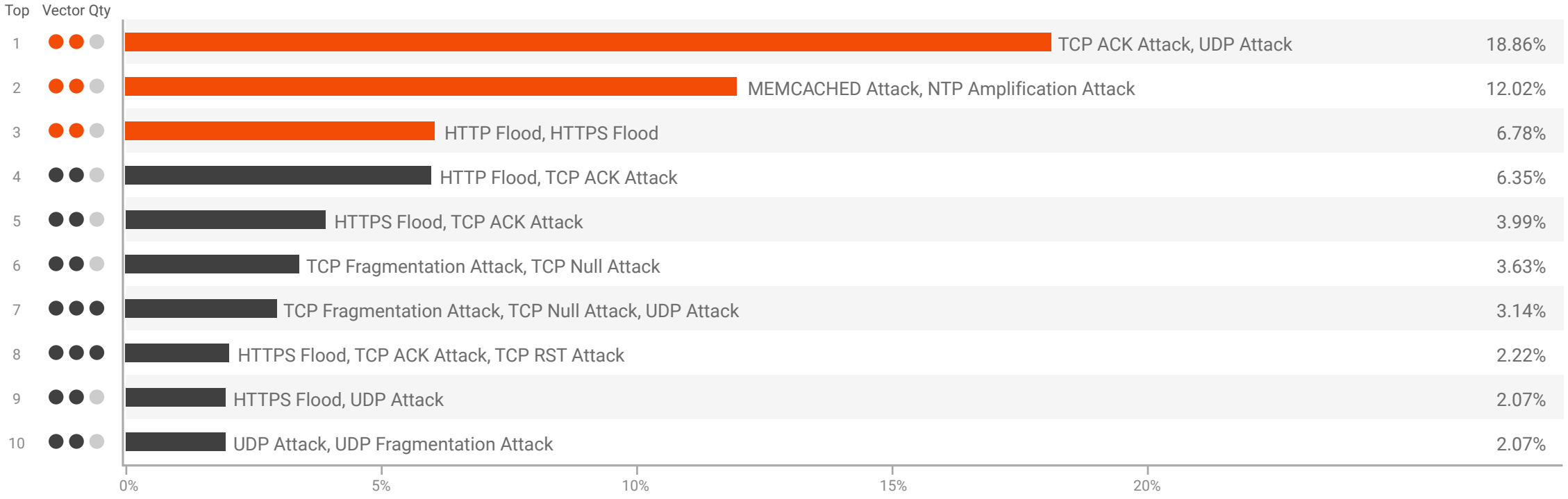


Figure 6 - Top 10 multi-vector combinations in 2022

2022 Attack Statistics

Attack Durations

Over 66% of attacks were shorter than 90 minutes, while the rest lasted longer than 90 minutes. 18.26% of attacks exceeded 1200 minutes. The average attack duration recorded in 2022 was 82.76 minutes, with the longest attack lasting 27642.12 minutes. Both the maximum and average duration increased by 79.40% and fell by 10.42% respectively, YoY.

66%

of attacks were shorter than 90 minutes

Duration (Minutes)	2021	2022
Maximum	15408.43	27642.12
Average	92.39	82.76

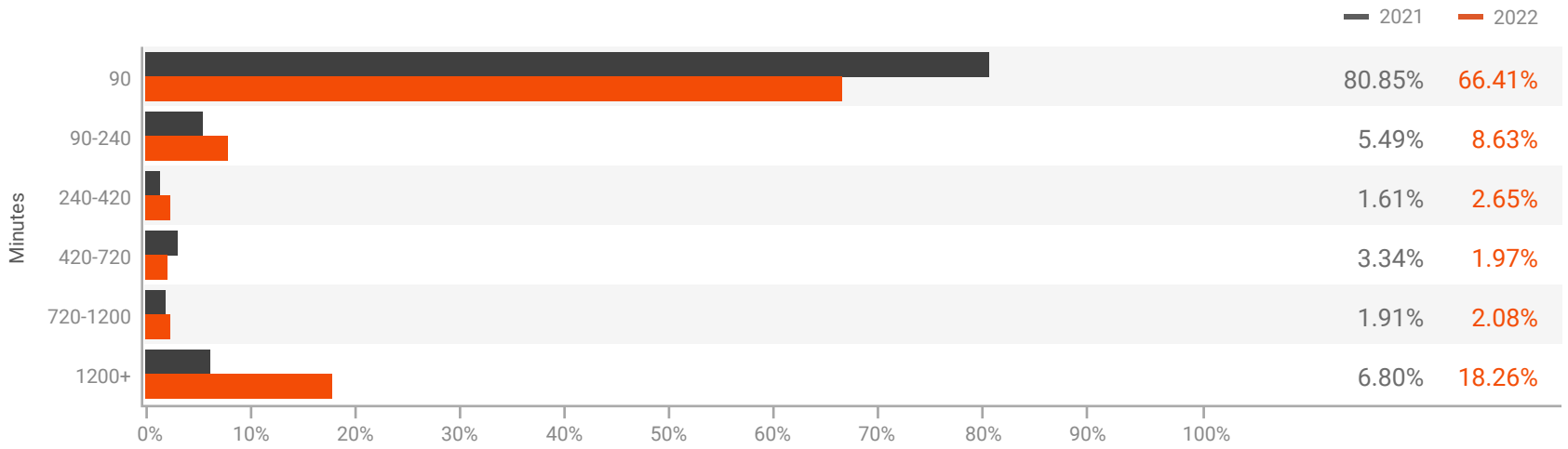


Figure 7 - Percentage Change of Attack Durations in 2021 and 2022

2022 Attack Statistics

Attack Size Distribution

Of the attacks recorded in 2022, 88.14% were smaller than 1Gbps. 11.68% ranged between 1Gbps - 10Gbps, and 0.18% were larger than 10Gbps.

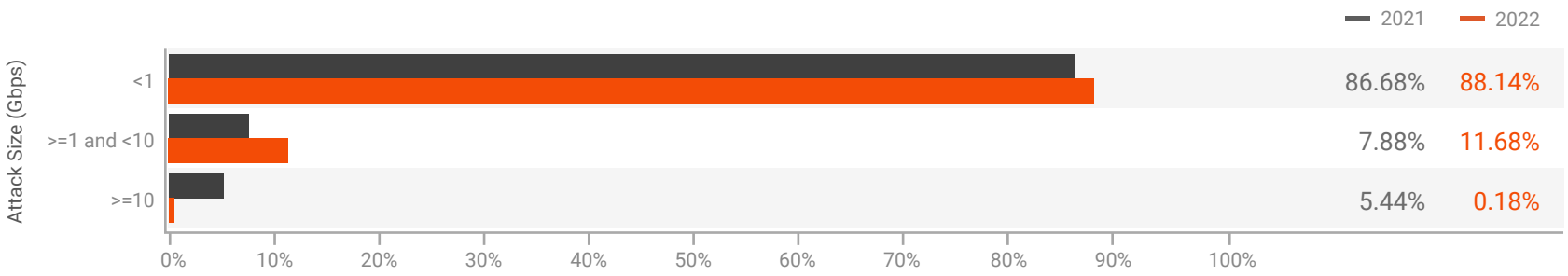


Figure 8 - Attack Size Distribution in 2021 and 2022

88%

of attacks were smaller than 1Gbps

2022 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.

Targeted ASNs

240

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

3,079

Summary 1 - Bit-and-Piece Attacks in 2021 and 2022

		2021	2022	Difference
No. of Targeted ASN		119	240	101.68%
No. Target Geolocations		28	20	-28.57%
Total IP prefixes under attack(Class C)		1,585	3,079	94.26%
No. of targeted IP addresses per IP prefix	Minimum	10	30	200.00%
	Maximum	256	256	0.00%
Attack Duration(Minutes)	Minimum	13.42	2.00	-85.10%
	Maximum	4,230.18	2,577.00	-39.08%
Attack Count per IP	Minimum	40	40	0.00%
	Maximum	765,002	74,570	-90.25%
Attack Count per IP Prefix	Minimum	513	441	-14.04%
	Maximum	1,821,606	3,366,723	84.82%
Attack Size by IP (Gbps)	Minimum	0.0001	0.0004	300.00%
	Maximum	101.13	21.38	-78.86%
Attack Size by IP Prefix /24 (Gbps)	Minimum	0.0002	0.0297	14,750.00%
	Maximum	295.83	123.72	-58.18%

Summary 2 - Bit-and-Piece Attack Types

2021	2022	
TCP ACK Attack(35.45%)	SSDP Amplification Attack(44.75%)	CLDAP Reflection Attack(0.27%)
UDP Fragmentation Attack(15.07%)	NTP Amplification Attack(20.14%)	HTTPS Flood(0.19%)
SSDP Amplification Attack(11.29%)	Memcached Attack(10.89%)	BITTORRENT Amplification Attack(0.19%)
CLDAP Reflection Attack(10.74%)	CHARGEN Attack(6.86%)	L2TP Amplification Attack(0.16%)
UDP Attack(8.60%)	UDP Fragmentation Attack(6.15%)	IP Fragmentation Attack(0.11%)
CHARGEN Attack(7.81%)	DNS Amplification Attack(2.50%)	DNS Attack(0.05%)
DNS Amplification Attack(6.66%)	UDP Attack(1.62%)	SIP Flood(0.03%)
ICMP Attack(1.74%)	TCP ACK Attack(1.59%)	
TCP SYN Attack(0.70%)	ICMP Attack(0.88%)	
IP Fragmentation Attack(0.40%)	TCP SYN Attack(0.69%)	
NTP Amplification Attack(0.35%)	SNMP Amplification Attack(0.52%)	
IP BOGONS(0.35%)	IP BOGONS(0.47%)	
TCP Null Attack(0.30%)	TCP RST Attack(0.44%)	
HTTPS Flood(0.20%)	TCP Null Attack(0.38%)	
TCP RST Attack(0.20%)	TCP Fragmentation Attack(0.38%)	
DNS Attack(0.10%)	HTTP Flood(0.36%)	
MDNS Amplification Attack(0.05%)	WS-DISCOVERY Amplification Attack(0.36%)	

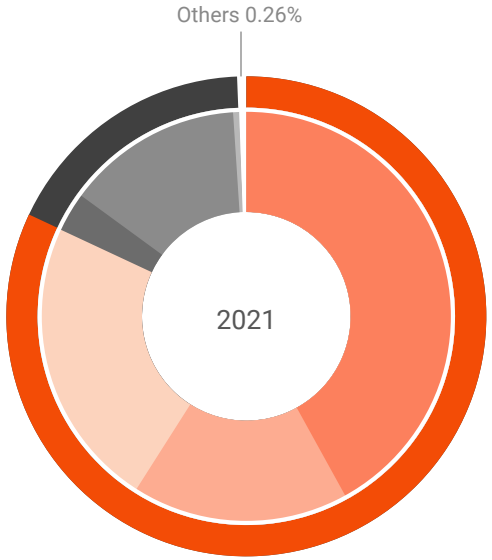
Summary 3 - Bit-and-Piece Targeted Geo-locations

2021	2022
Argentina, Austria, Bangladesh, Brazil, Bulgaria, Chile, China, Colombia, Czechia, France, Germany, Hong Kong, India, Indonesia, Israel, Norway, Pakistan, Philippines, Seychelles, Singapore, SouthAfrica, Sri Lanka, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Kingdom, United States	Argentina, Bangladesh, Brazil, Chile, Czechia, Germany, Hong Kong, Indonesia, Paraguay, Philippines, Russian Federation, Singapore, South Korea, Spain, Taiwan, Thailand, Turkey, United Arab Emirates, United States, Vietnam

2022 Attack Statistics

Source Distribution of Application Attacks[1]

MacOS devices contributed to 8.71% of all application attack traffic, while Windows-powered PCs and notebooks contributed 15.42%. Mobile iOS devices such as iPads and iPhones made up 2.25% of all application attack traffic, whereas android devices accounted for 65.53%.



Source Distribution of Application Attacks

	2021	2022
Computers and Servers	**81.92%**	**31.98%**
Windows OS	41.99%	15.42%
Macintosh OS	17.07%	8.71%
Other OS	22.86%	7.85%
Mobile Devices	**17.82%**	**67.88%**
iOS	3.37%	2.25%
Android	14.32%	65.53%
BlackBerry, DoCoMo	0.13%	0.10%
Others Other OS e.g. PSP, Nintendo Wii, Nintendo DS	**0.26%**	**0.14%**

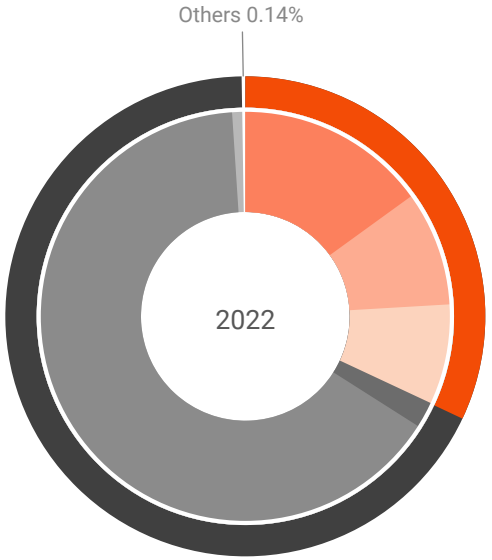


Figure 9 - Source Distribution of Application Attacks in 2021 and 2022

Change in Attack Surfaces

Attack surfaces change often. If a hacker team has little success in launching DDoS against a specific hosting or CSP, they will pivot their attacks looking to better-expected results.

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.

2022 Attack Statistics

Application Attack Source Distribution (IP Reputation)

Top 10 Attack Sources Ranking in 2022

	2022
Thailand	32.23%
China	22.75%
United States	9.65%
Brazil	8.81%
Turkey	6.12%
Singapore	2.34%
India	2.06%
Indonesia	2.01%
Hong Kong	1.58%
Malaysia	1.24%
Others	11.21%

Top 10 Attack Sources Ranking in APAC (2022)

	2022
Thailand	47.48%
China	33.52%
Singapore	3.44%
India	3.04%
Indonesia	2.96%
Hong Kong	2.32%
Malaysia	1.82%
Australia	1.81%
Philippines	1.19%
Japan	0.62%
Others	1.79%

Top 10 Attack Sources Ranking in Europe (2022)

	2022
Ireland	20.08%
United Kingdom	16.04%
Germany	12.40%
Russian Federation	11.48%
France	6.39%
Netherlands	5.84%
Ukraine	2.93%
Italy	2.50%
Spain	2.41%
Norway	2.15%
Others	17.77%

Rise of Botnets & DDoS Attacks in the Tech World

Those who control botnets are commonly referred to as botmasters.

Botnets can be used to launch DDoS attacks on the Internet. These botnets target IoT devices, servers, and workstations. Attackers can still launch attacks without having their botnets by manipulating millions of Internet devices. It is essential to understand how botnets are being exploited.

Top 10 Attack Sources Ranking in Middle East and Africa (2022)

	2022
Turkey	88.63%
Iran	3.71%
Kenya	0.91%
South Africa	0.86%
Saudi Arabia	0.80%
Uganda	0.67%
Nigeria	0.66%
Egypt	0.54%
United Arab Emirates	0.43%
Yemen	0.29%
Others	2.51%

Top 10 Attack Sources Ranking in America (2022)

	2022
United States	45.20%
Brazil	41.24%
Mexico	2.14%
Canada	1.76%
Argentina	1.52%
Dominican Republic	1.08%
Ecuador	1.00%
El Salvador	0.98%
Colombia	0.75%
Costa Rica	0.69%
Others	3.64%

2022 Attack Statistics

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

Top 10 ASN Attacks Ranking (2022)

	AS Name	2022
4134	Chinanet	8.41%
16509	AMAZON-02	6.28%
4837	CHINA UNICOM China169 Backbone	5.58%
9808	China Mobile Communications Group Co., Ltd.	4.60%
24940	Hetzner Online GmbH	2.38%
37963	Hangzhou Alibaba Advertising Co.,Ltd.	1.84%
15897	Vodafone Telekomunikasyon A.S.	1.82%
16135	Turkcell Iletisim Hizmetleri A.s.	1.75%
17547	M1 NET LTD	1.71%
45090	Shenzhen Tencent Computer Systems Company Limited	1.47%
Other		64.16%

Top 10 ASN Attacks Ranking in APAC (2022)

	AS Name	2022
4134	Chinanet	17.26%
4837	CHINA UNICOM China169 Backbone	11.45%
9808	China Mobile Communications Group Co., Ltd.	9.44%
37963	Hangzhou Alibaba Advertising Co.,Ltd.	3.79%
17547	M1 NET LTD	3.50%
45090	Shenzhen Tencent Computer Systems Company Limited	3.01%
4760	HKT Limited	2.55%
9381	HKBN Enterprise Solutions HK Limited	1.72%
9269	Hong Kong Broadband Network Ltd.	1.70%
45102	Alibaba US Technology Co., Ltd.	1.68%
Others		43.90%

Top 10 ASN Attacks Ranking in Europe (2022)

	AS Name	2022
24940	Hetzner Online GmbH	17.70%
31083	Telepoint Ltd	8.15%
9009	M247 Ltd	8.06%
16276	OVH SAS	4.51%
49981	WorldStream B.V.	4.19%
206512	Tigova Network Limited	4.17%
13188	Content Delivery Network Ltd	4.16%
9009	M247 Europe SRL	2.20%
212238	Datacamp Limited	1.84%
25500	User Association of Ukrainian Research and Academic Network URAN	1.62%
Others		43.42%

Top 10 ASN Attacks Ranking in Middle East and Africa (2022)

	AS Name	2022
15897	Vodafone Telekomunikasyon A.S.	18.38%
16135	Turkcell Iletisim Hizmetleri A.s.	17.68%
9121	Turk Telekom	14.80%
20978	TT Mobil Iletisim Hizmetleri A.S	13.03%
34984	Superonline Iletisim Hizmetleri A.S.	6.45%
47331	Turk Telekom	5.02%
8386	Vodafone Net Iletisim Hizmetleri Anonim Sirketi	3.70%
12978	Andromeda Tv Digital Platform Isletmeciligi A.s.	3.28%
47524	Turksat Uydu Haberlesme ve Kablo TV Isletme A.S.	3.14%
12735	TurkNet Iletisim Hizmetleri A.S.	2.35%
Others		12.16%

Top 10 ASN Attacks Ranking in America (2022)

	AS Name	2022
16509	AMAZON-02	22.53%
14061	DIGITALOCEAN-ASN	4.19%
26615	TIM SA	3.15%
28573	Claro NXT Telecomunicacoes Ltda	3.10%
16397	EQUINIX BRASIL	2.98%
33387	NOCIX	2.51%
18450	WEBNX	2.23%
8075	MICROSOFT-CORP-MSN-AS-BLOCK	1.51%
7738	V tal	1.30%
27699	TELEFONICA BRASIL S.A	1.23%
Others		55.26%

2022 Attack Statistics

Reflected Attack Destination Distribution

Top 10 Reflected Attack Destinations around the globe (2022)

	Percentage
Brazil	59.08%
South Korea	19.87%
United States	4.93%
China	4.33%
Indonesia	1.31%
United Kingdom	1.16%
Hong Kong	0.90%
Ecuador	0.82%
Russian Federation	0.69%
Germany	0.63%
Others	6.30%

Top 10 Reflected Attack Destinations in APAC (2022)

	Percentage
South Korea	72.51%
China	15.79%
Indonesia	4.77%
Hong Kong	3.28%
Australia	0.97%
Singapore	0.70%
Taiwan	0.66%
Bangladesh	0.35%
Vietnam	0.26%
India	0.23%
Others	0.48%

Top 10 Reflected Attack Destinations in Europe (2022)

	Percentage
United Kingdom	22.72%
Russian Federation	13.58%
Germany	12.30%
Kazakhstan	8.25%
France	7.58%
Netherlands	7.45%
Czechia	4.92%
Spain	4.31%
Poland	2.43%
Romania	2.08%
Others	14.39%

Top 10 Reflected Attack Destinations in Middle East and Africa (2022)

	Percentage
Turkey	23.33%
Saudi Arabia	22.18%
Seychelles	20.55%
Iran	15.00%
United Arab Emirates	4.45%
Kuwait	4.03%
Iraq	3.68%
South Africa	2.17%
Qatar	0.69%
Mauritius	0.67%
Others	3.26%

Top 10 Reflected Attack Destinations in America (2022)

	Percentage
Brazil	89.61%
United States	7.47%
Ecuador	1.24%
Canada	0.66%
Paraguay	0.35%
Argentina	0.25%
Mexico	0.17%
Costa Rica	0.09%
Chile	0.07%
Colombia	0.02%
Others	0.06%

Upcoming Major DDoS Trends

DDoS Attacks Against Internet of Things Devices

IoTs can be helpful for users and prevent DDoS attacks. However, this is only sometimes the case for IoT devices. They have large attack surfaces and often overlook security principles in their designs. Some widgets have let attackers log in. Users may need help changing their IDs sometimes.

AI-Powered DDoS Attack Vectors

As the world celebrated the rise of ChatGPT and other artificial intelligence and machine learning capabilities, hacker equality continued to invest in the same functionality. Hackers, along with global organizations, recruit AI and ML engineers. Often hackers and international organizations are competitors for the same talent pool.

Global organizations recognize the value of AI and the ability to process and rationalize data. Hackers see the value of processing past or present DDoS attack forensics and leverage AI and ML to predict a successful future attack.

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 Annual Statistical Report.

20230601-EN

About Nexusguard

Founded in 2008, Nexusguard is a leading 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