Distributed Denial of Service (DDoS)

DDoS Statistical Report 1HY 2022

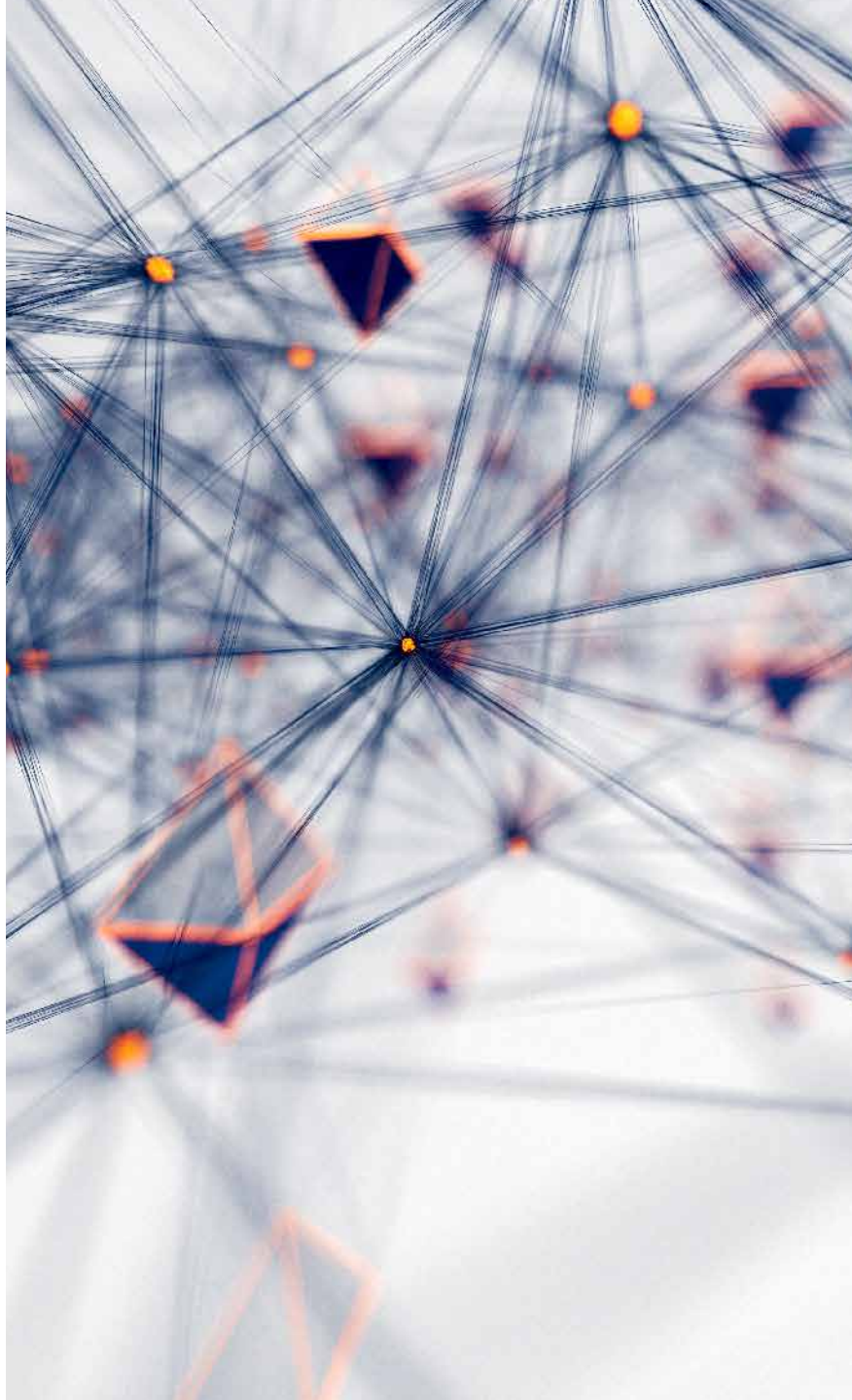
NEXUSGUARD®

Table of Contents

Key Observations for First Half Year of 2022

- In the first half of 2022, the total attack count and average attack size increased by 75.60% and decreased by 55.97% respectively compared to the figures recorded in the second half of 2021.
- Compared to the second half of 2021, the maximum attack size decreased by 66.82%, with the maximum attack size clocking in at 232.00 Gbps.
- UDP based attacks in the first half of 2022 increased by 77.53% compared to the second half of 2021.
- Application attacks increased by 330.00% HoH[1], while Amplification attacks increased by 106.65% in the same period.

1 HoH stands for Half on Half (comparative of results for 1HY 2022 vs. 2HY 2021)



Key Observations for First Half Year of 2022

Metrics

Total Attacks

vs. 2021 Second Half

75.60% ▲

vs. 2021 First Half

-9.92% ▼

Attack Sizes

Maximum

232.00 Gbps

vs. 2021 Second Half

-66.82% ▼

vs. 2021 First Half

-23.08% ▼

Average

0.59 Gbps

vs. 2021 Second Half

-55.97% ▼

vs. 2021 First Half

47.50% ▲

DDoS Attack Types

vs. 2021 Second Half

UDP Attack	HTTPS Flood	TCP ACK Attack	Volumetric (Direct Flood)	Application Attack	Volumetric (Amplification)
56.76% ▲	75.95% ▲	-63.86% ▼	48.22% ▲	330.00% ▲	106.65% ▲

vs. 2021 First Half

UDP Attack	HTTPS Flood	TCP ACK Attack	Volumetric (Direct Flood)	Application Attack	Volumetric (Amplification)
-18.39% ▼	692.39% ▲	14.21% ▲	-15.06% ▼	734.87% ▲	-49.71% ▼

Key Observations for First Half Year of 2022

Trends

Compared to the same period over a 5 year span, March recorded the lowest number of attacks, while June registered the highest number of attacks as well as the highest attack count in the 1HY 2022 period. While the number of attacks increased from April 2022 to June 2022, there was a drop in attack count during the same period in 2021.

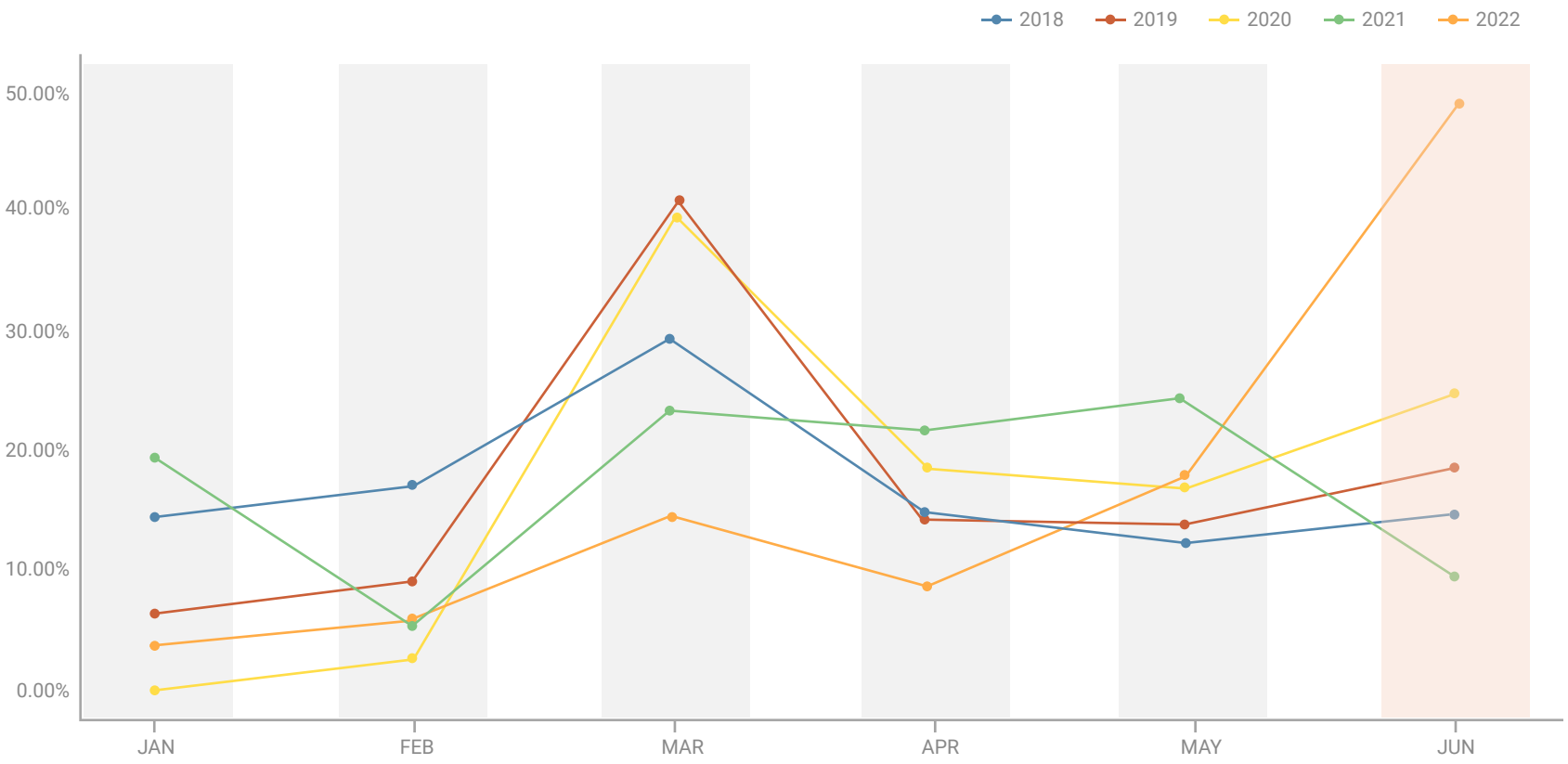


Figure 1 - DDoS Attack Trends from 2018 - 2022

First Half of 2022 Attack Statistics

NEXUSGUARD®

First Half of 2022 Attack Statistics

Types of Attack Vectors

In the first half of 2022, UDP Attack and HTTPS Flood were the predominant two attack types, contributing 39.58% and 15.94% respectively, while TCP ACK Attacks ranked third at 6.48%.

The number of UDP Attacks increased by 56.76% HoH and decreased by 18.39% YoY, while HTTPS Flood attacks increased by 75.95% HoH and a whopping 692.39% YoY.

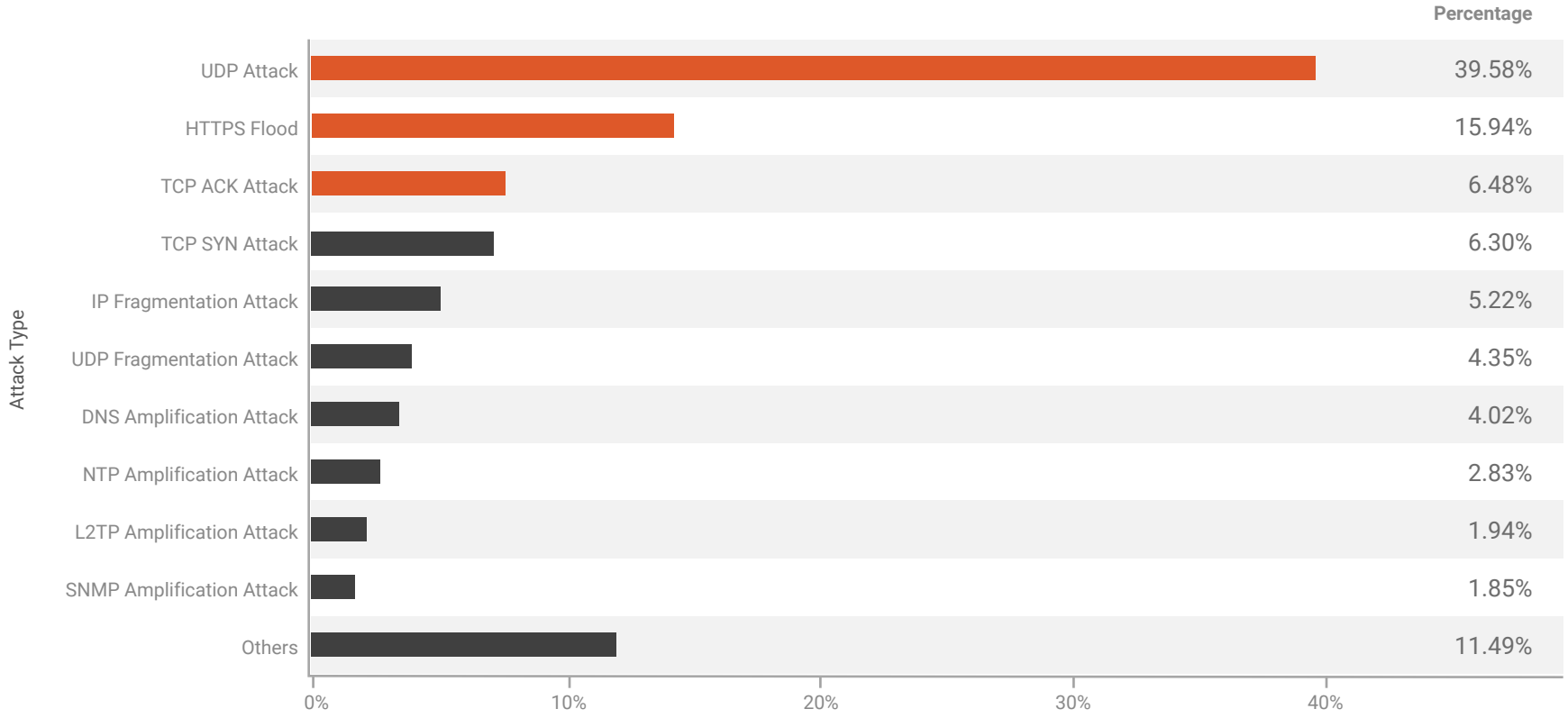


Figure 2 - Top 10 Attack Vectors in 1HY 2022

First Half of 2022 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 HTTPS Flood

Attackers attempt to exhaust server resources by generating valid, volumetric HTTPS requests or sessions. The sessions are typically HTTPS GET, which overwhelm the victim's web servers by flooding them with answer requests (ACK). The process forces servers to allocate maximum resources to handle the volumetric attack traffic. As a result, legitimate requests cannot get through.

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.

First Half of 2022 Attack Statistics

Attacks by Category

Volumetric (Direct Flood) attacks, contributing 67.93% of the total attacks recorded in the first half of 2022, increased by 48.22% HoH and decreased by 15.06% YoY, while Application attacks contributing 17.51%, increased by 330.00% and 734.87% HoH and YoY respectively. Volumetric (Amplification) attacks representing 14.56% of the attacks in the first half year of 2022, grew by 106.65% HoH and dropped by 49.71% YoY.

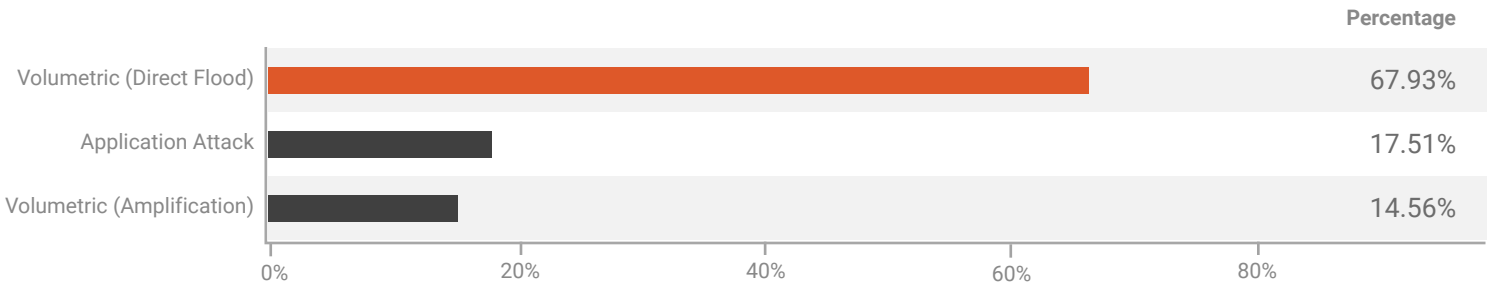


Figure 3 - Distribution of Attacks by Category in 1HY 2022

Direct Flood attacks

+48%

Application attacks

+330%

Amplification attacks

+106%

First Half of 2022 Attack Statistics

Attacks by Protocol

UDP and TCP based attacks were the predominant two attack types in the first half of 2022, contributing 61.27% and 30.57% respectively. The number of UDP based attacks rose by 77.53% HoH and fell by 26.93% YoY, while TCP based attacks increased by 67.97% and 34.13% HoH and YoY respectively.

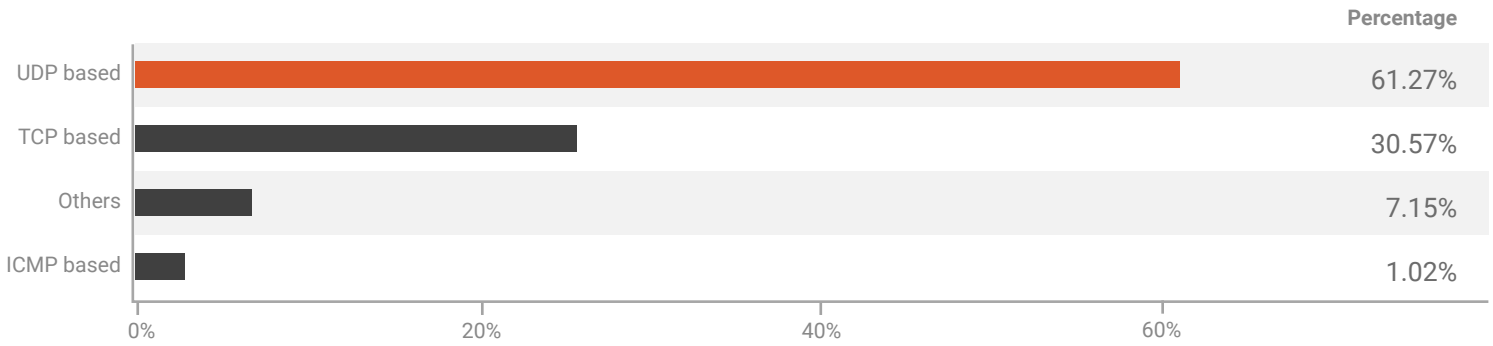


Figure 4 - Distribution of Attacks by Protocols in 1HY 2022

UDP based attacks

+78%

TCP based attacks

+68%

First Half of 2022 Attack Statistics

Quantity of Attack Vectors

Single-vector attacks played the leading role in the first half of 2022. 85.37% of attacks were single vector, while the rest were multi-vector.

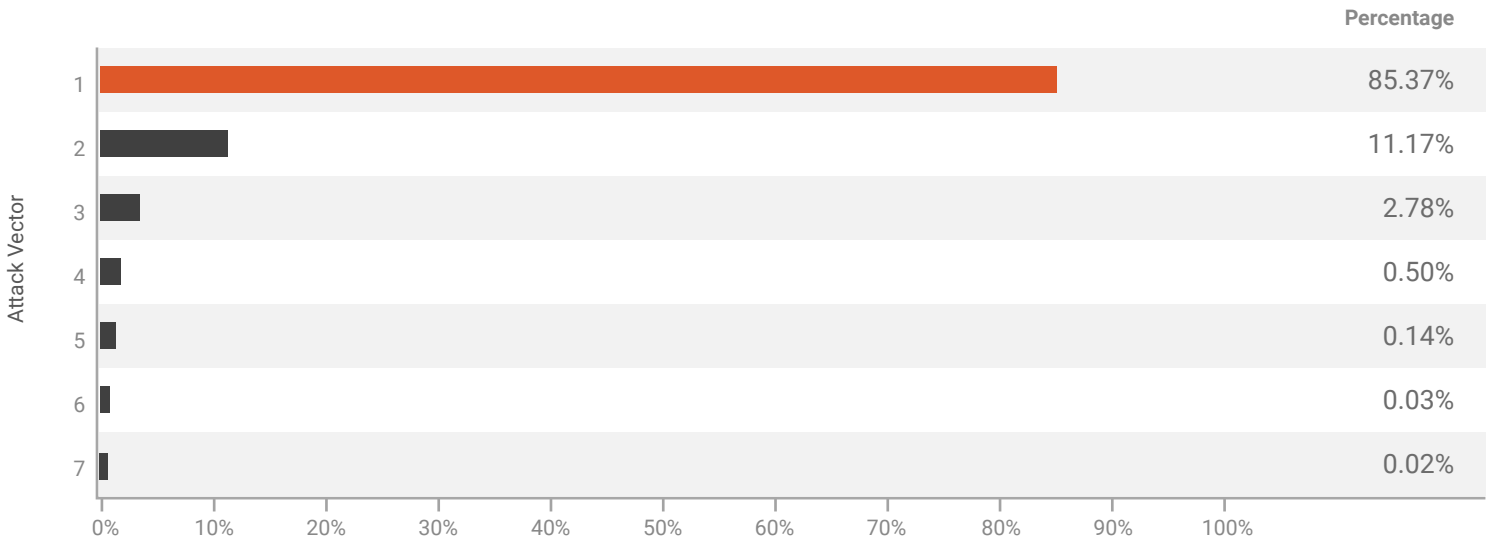


Figure 5 - Distribution of DDoS Attack Vectors in 1HY 2022

Single-vector attacks

85%

Multi-vector attacks

15%

First Half of 2022 Attack Statistics

Multi-Vector Attack Combinations

The most commonly used multi-vector attack combination recorded in the first half of 2022 was “TCP ACK Attack, UDP Attack”, contributing 30.72%
In second place was a combination of “TCP Fragmentation Attack, TCP Null Attack”, contributing 7.53%.
And third place was made up of “TCP Fragmentation Attack, TCP Null Attack, UDP Attack”, contributing 7.36%.

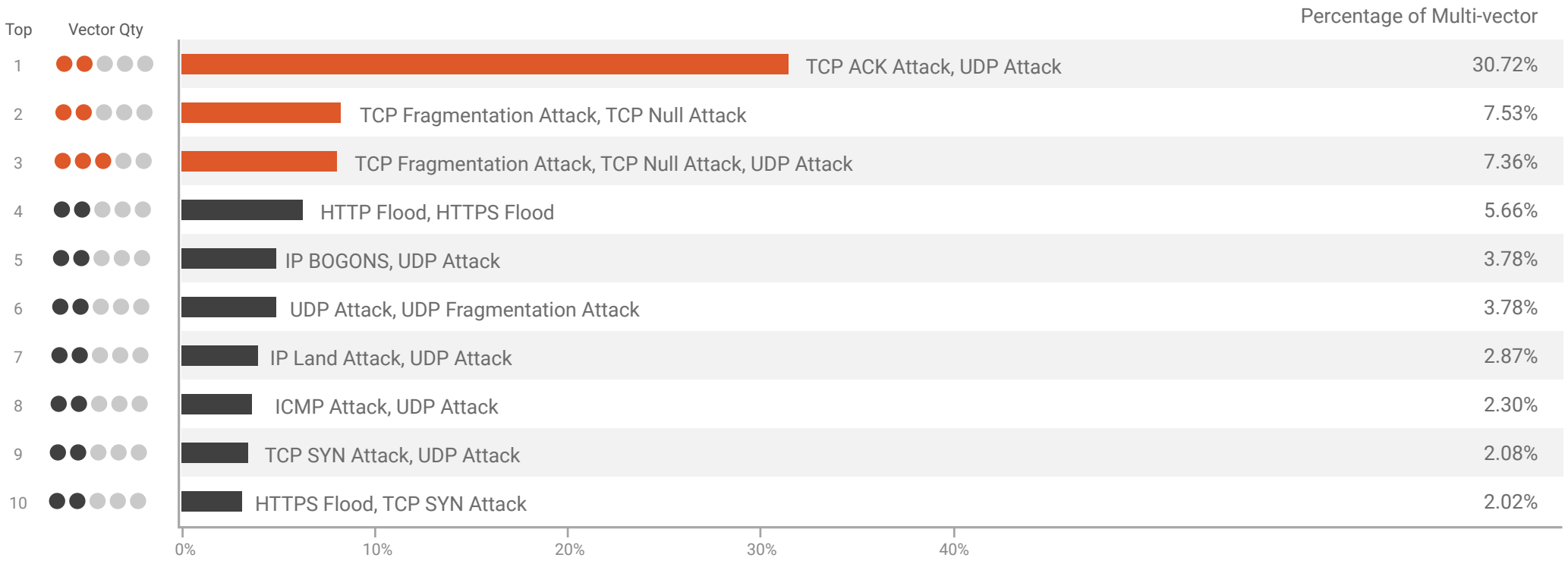


Figure 6 - Top 10 multi-vector combinations in 1HY 2022

First Half of 2022 Attack Statistics

Attack Durations

69.27% of attacks were shorter than 90 minutes, while the rest lasted longer than 90 minutes. 17.15% of attacks exceeded 1200 minutes.
The average attack duration recorded in the first half of 2022 was 90.97minutes, with the longest attack lasting 27642.12 minutes.
The maximum duration increased by 113.98% and 79.40% HOH and YoY respectively, while the average duration decreased by 45.40% and 26.69% HoH and YoY respectively.

69%

of attacks were shorter than 90 minutes

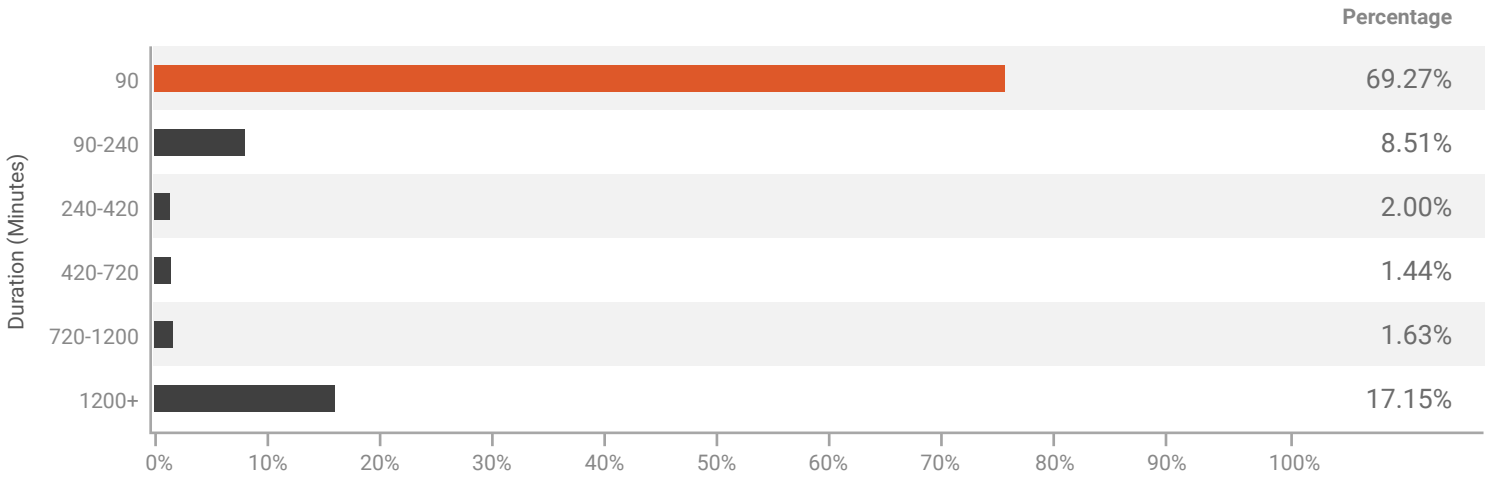


Figure 7 - Percentage Change of Attack Durations in 1HY 2022

First Half of 2022 Attack Statistics

Attack Size Distribution

Of the attacks recorded in the first half of 2022, 81.77% were smaller than 1Gbps. 18.06% ranged between 1Gbps - 10Gbps, and 0.18% were larger than 10Gbps.

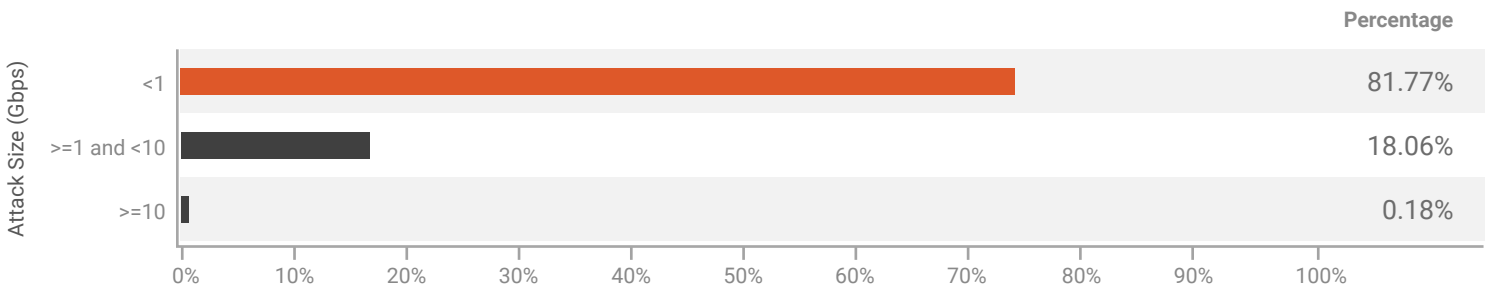


Figure 8 - Attack Size Distribution in 1HY 2022

81%

of attacks were smaller than 1Gbps

First Half of 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

77

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

734

Summary 1 - Bit-and-Piece Attacks

	Minimum	Maximum
No. of targeted IP addresses per /24 network	10	256
Attack Size by IP (Gbps)	0.0004	13.13
Attack Size by /24 network (Gbps)	0.0637	123.72
Average Attack Size(Gbps)	Less than 0.0001	0.15
Attack count per IP	40	74570
Attack count per IP prefix	1585	3366723
Duration (minutes)	13.00	2577.00

Summary 2 - Bit-and-Piece Attacks Types

	Percentage
SSDP Amplification Attack	35.38%
CHARGEN ATTACK	25.60%
UDP Fragmentation Attack	6.78%
DNS Amplification Attack	6.15%
UDP Attack	5.27%
TCP ACK Attack	4.27%
ICMP Attack	3.26%
NTP Amplification Attack	2.63%
SNMP Amplification Attack	2.38%
IP BOGONS	1.88%
TCP SYN Attack	1.88%
TCP Null Attack	1.13%
TCP Fragmentation Attack	0.88%
BITTORRENT Amplification Attack	0.88%
L2TP Amplification Attack	0.63%
Memcached Attack	0.38%
DNS Attack	0.25%
IP Fragmentation Attack	0.13%
CLDAP Reflection Attack	0.13%
STEAM PROTOCOL Amplification Attack	0.13%

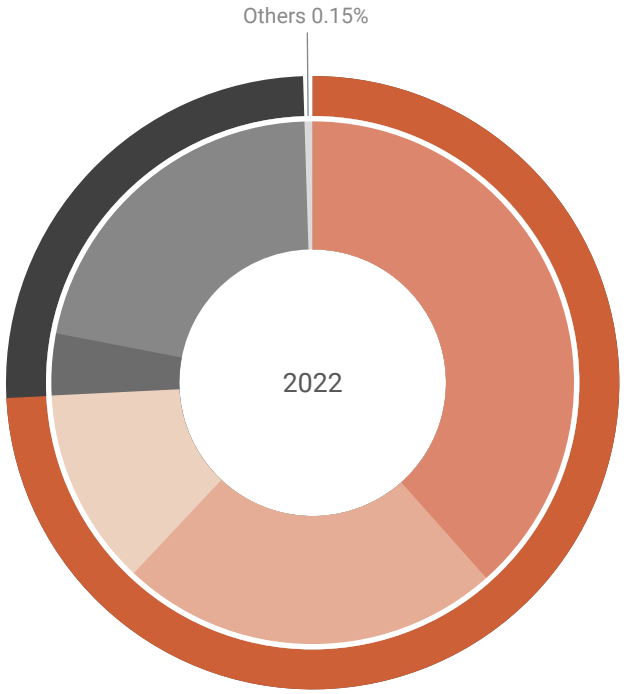
Summary 3 - Bit-and-Piece Targeted Geo-locations

Argentina, Bangladesh, Brazil, Chile, Germany, Hong Kong, Paraguay, Philippines, Singapore, Thailand, United Arab Emirates, United States

First Half of 2022 Attack Statistics

Source Distribution of Application Attacks[2]

MacOS devices contributed to 23.49% of all application attack traffic, while Windows-powered PCs and notebooks contributed 38.48%. Mobile iOS devices such as iPads and iPhones made up 3.87% of all application attack traffic, whereas android devices accounted for 21.66%.



Source Distribution of Application Attacks

	Percentage
Computers and Servers	**74.26%**
Windows OS	38.48%
Macintosh OS	23.49%
Other OS	12.29%
Mobile Devices	**25.60%**
iOS	3.87%
Android	21.66%
BlackBerry, DoCoMo	0.07%
Others	**0.15%**

Figure 9 – Source Distribution of Application Attacks in 1HY 2022

2 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.

First Half of 2022 Attack Statistics

Application Attack Source Distribution (IP Reputation)

Top Ten Source Ranking around the globe (1HY 2022)

	Percentage
Thailand	34.51%
United States	13.21%
China	12.55%
Turkey	6.79%
Singapore	5.49%
Indonesia	4.67%
India	3.17%
Hong Kong	3.00%
Brazil	2.62%
Malaysia	1.76%
Others	12.24%

Top Ten Sources Ranking in APAC (1HY 2022)

	Percentage
Thailand	49.09%
China	17.86%
Singapore	7.81%
Indonesia	6.64%
India	4.51%
Hong Kong	4.26%
Malaysia	2.50%
Australia	2.48%
Philippines	1.81%
Vietnam	0.76%
Others	2.27%

Top Ten Sources Ranking in Europe (1HY 2022)

	Percentage
United Kingdom	18.23%
Germany	14.20%
Russian Federation	12.15%
France	9.42%
Ireland	8.18%
Netherlands	5.92%
Norway	3.77%
Ukraine	3.36%
Italy	2.58%
Spain	2.38%
Others	19.80%

Top Ten Sources Ranking in Middle East and Africa (1HY 2022)

	Percentage
Turkey	86.73%
Iran	3.71%
Kenya	1.63%
Uganda	1.31%
Nigeria	0.91%
South Africa	0.88%
Egypt	0.79%
Saudi Arabia	0.55%
Sierra Leone	0.40%
United Arab Emirates	0.37%
Others	2.73%

Top Ten Sources Ranking in America (1HY 2022)

	Percentage
United States	76.66%
Brazil	15.20%
Canada	3.27%
Mexico	1.21%
Argentina	0.84%
El Salvador	0.46%
Bolivia	0.34%
Ecuador	0.32%
Colombia	0.31%
Costa Rica	0.24%
Others	1.16%

First Half of 2022 Attack Statistics

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

Top Ten Attack Source by ASN around the globe (1HY 2022)

ASN	AS Name	Percentage
4134	CHINANET-BACKBONE	7.83%
16509	AMAZON-02	4.18%
4837	CHINA169-BACKBONE	3.53%
9808	CHINAMOBILE-CN	3.32%
14061	DIGITALOCEAN-ASN	3.30%
9009	M247	3.26%
24940	HETZNER-AS	2.97%
37963	ALIBABA-CN-NET	2.63%
17547	M1NET-SG-AP	2.33%
45090	TENCENT-NET-AP	2.27%
Others		64.38%

Top Ten Attack Sources by ASN in APAC (1HY 2022)

ASN	AS Name	Percentage
4134	CHINANET-BACKBONE	17.50%
4837	CHINA169-BACKBONE	7.89%
9808	CHINAMOBILE-CN	7.43%
37963	ALIBABA-CN-NET	5.89%
17547	M1NET-SG-AP	5.21%
45090	TENCENT-NET-AP	5.07%
4760	HKTIMS-AP	2.64%
9269	HKBN-AS-AP	2.36%
56040	CMNET-GUANGDONG-AP	2.33%
9381	HKBNES-AS-AP	2.16%
Others		41.52%

Top Ten Attack Sources by ASN in Europe (1HY 2022)

ASN	AS Name	Percentage
9009	M247	13.08%
24940	HETZNER-AS	11.93%
31083	TELEPOINT	5.43%
13188	TRIOLAN	4.27%
25500	NTUU-KPI-AS	3.21%
16276	OVH	3.15%
15895	KSNET-AS	2.66%
212238	CDNEXT	2.48%
206512	TIGOVA	2.21%
39608	LANETUA-AS	2.16%
Others		49.43%

Top Ten Attack Sources by ASN in Middle East and Africa (1HY 2022)

ASN	AS Name	Percentage
15897	VODAFONETURKEY	16.89%
16135	TURKCELL-AS	16.84%
9121	TTNET, TR	14.34%
20978	TT_MOBIL	12.23%
34984	TELLCOM-AS	8.60%
47331	TTNET	4.82%
12978	DSMART	4.55%
8386	KOCNET	3.81%
47524	TURKSAT-AS	3.57%
12735	ASTURKNET	2.24%
Others		12.12%

Top Ten Attack Sources by ASN in America (1HY 2022)

ASN	AS Name	Percentage
16509	AMAZON-02	18.97%
14061	DIGITALOCEAN-ASN	14.96%
8075	MICROSOFT-CORP-MSN-AS-BLOCK	3.40%
174	COGENT-174	2.54%
13335	CLOUDFLARENET	2.53%
28573	Claro NXT Telecomunicacoes Ltda	2.51%
31898	ORACLE-BMC-31898	2.16%
14754	Telgua	1.68%
53667	PONYNET	1.66%
396982	GOOGLE-CLOUD-PLATFORM	1.63%
Others		47.95%

First Half of 2022 Attack Statistics

Reflected Attack Destinations

Top Ten Reflected Attack Destinations around the globe (1HY 2022)

	Percentage
Brazil	40.60%
South Korea	34.01%
China	6.03%
United States	5.99%
Ecuador	1.67%
United Kingdom	1.53%
Kazakhstan	0.83%
Russian Federation	0.73%
Canada	0.67%
Seychelles	0.63%
Others	7.30%

Top Ten Reflected Attack Destinations in APAC (1HY 2022)

	Percentage
South Korea	81.46%
China	14.44%
Australia	0.91%
Singapore	0.73%
Hong Kong	0.68%
Bangladesh	0.41%
Taiwan	0.38%
Vietnam	0.24%
India	0.22%
Malaysia	0.20%
Others	0.33%

Top Ten Reflected Attack Destinations in Europe (1HY 2022)

	Percentage
United Kingdom	24.64%
Kazakhstan	13.37%
Russian Federation	11.74%
Germany	9.97%
France	9.63%
Netherlands	8.16%
Romania	2.70%
Poland	2.14%
Portugal	1.68%
Austria	1.58%
Others	14.39%

Top Ten Reflected Attack Destinations in Middle East and Africa (1HY 2022)

	Percentage
Seychelles	29.68%
Saudi Arabia	25.80%
Iran	15.84%
United Arab Emirates	5.91%
Kuwait	5.57%
Turkey	4.54%
Iraq	4.50%
South Africa	2.35%
Iran	2.06%
Qatar	0.88%
Others	2.87%

Top Ten Reflected Attack Destinations in America (1HY 2022)

	Percentage
Brazil	81.34%
United States	12.01%
Ecuador	3.35%
Canada	1.34%
Paraguay	0.94%
Argentina	0.37%
Mexico	0.35%
Chile	0.16%
Costa Rica	0.04%
Colombia	0.03%
Others	0.07%

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 Half-Year Statistical Report.

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