Summary of DDoS Industry Reports 2022

VENDOR	SUMMARY	TITLE	FORMAT	PERIOD	ATTACK COUNTS	R/A	D/P	VECTORS	CHANGES END OF 2022	ATTACK DURATION/SIZE	ATTACK INTENSITY	CARPET BOMBING/PREFIX	MULTI-VECTOR	TARGET	VANTAGE POINTS/SOURCES
A10	DDoS landscape in 2022. Focuses on the number of "weapons", not attacks themselves.	2022 DDoS Threat Report	Form/PDF	2019 up to **2021 2H**	No information about attack counts	p8: ⬆161% R/A **hosts** and DDoS **bots**. p21: SSDP	No specific information about direct/path attacks and associated vectors.	p9: largest DDoS "weapons" (reflectors, bots): SSDP 2.92M, PORTMAP 2M, SNMP 1.88M, DNS resolvers: 1.59M	Ends 2021	No information about attack duration.	Report makes a link between the attack intensity or destructive impact and the number of "weapons"	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	p5: Russia-Ukraine	p7: "A10 Networks' security research team gathers weapons intelligence by closely monitoring attack agents under the control of botnet command and control (C2); discovering malware innovations by deploying honeypots; intercepting self-replicating botnets; and scanning the internet for exposed reflected amplification sources."
Akamai	DDoS landscape in 2022	DDoS Attacks in 2022: Targeting Everything Online, All at Once	Open/Web	2022	No information about attack counts	Fig. 3: "most common attack vectors targeting tcp:80, tcp:443, port 53, and port >1000." *In our opinion, this seems incorrect, although any IP can be attacked using almost any protocol and port, it does not seem feasible to attack tcp:80 using UDP, or TCP with a different port.*	In Fig.3, "UDP flood" is listed as 15.7% of attacks against TCP:443, as well as other UDP-based vectors. *We believe this classification does not make sense.*		"In recent months, we've observed a surge in horizontal attacks (Figure 1)." Carpet-bombing.	No information about attack duration.	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	Fig 1: per quarter. Emphasis on carpet-bombing: "Horizontal attacks refer to simultaneous DDoS attacks aimed at multiple, unrelated targets (which is why they're sometimes called carpet bomb attacks)." "In recent months, we've observed a surge in horizontal attacks" "which hit 1813 IP addresses distributed across six physical data centers,"	Fig 3 has 4 pie charts that show the fraction of vectors used, depending on the targeted IP:port. There are no comments about potential overlap of vectors in attacks.	No information about targets, such as Industries, regions or countries affected.	"By analyzing the flow of data traversing our network, we can gain valuable insight into an IP's activities prior to an attack, which we refer to internally as its "IP day job.”"
Akamai	10y evolution of DDoS vectors, with a graph showing the fractions of vectors used in attacks	The Relentless Evolution of DDoS Attacks	Open/Web	2010-2022 (2022-05)	No information about attack counts	"Fig. 4: CharGEN attacks, SSDP floods, and CLDAP reflections are rarely seen today" NTP reflection 10.7%	Fig. 2: "UDP floods, SYN floods, and UDP fragmentation... They continue to be seen in force, often alongside other vectors." Fig. 5: 2022 (D/P) vectors: UDP flood 14.8%, UDP fragment 13.9%, SYN flood 9.2%, ACK flood 5.4%, DNS flood 5.3%	Fig. 1 represents the use of vectors through time; a long list of vectors.	Ends 2022-05	No information about attack duration.	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	No information about attacks with carpet-bombing.	Mentions the use of multiple vectors together	No information about targets, such as Industries, regions or countries affected.	No information about sources or methodology used.
Arelion	DDoS landscape in 2022, slide-based style	DDoS Threat Landscape Report 2023	Open/PDF	2022	p5: "The number of DDoS attacks in our global network decreased by a 1/3 in 2022 – with 50% fewer attacks towards our customers."	p11: " As a result [of reduction of spoofing], the **underlying threat from reflection attacks is slowly but surely being reduced**." p11: "DNS & NTP are still the two most common attack vectors, with NTP decreasing slightly during the year. "	p14: "we are seeing an increase in direct-path attacks from botnets, – albeit it to a lesser extent. These are more expensive to purchase since bots are a valuable asset for cyber criminals and if exposed, they risk being shut down when used extensively. Also, proxies are being used more – as a smoke screen to protect the bots from being exposed." *It is not clear if the increase is of D/P attacks, or D/P attacks from botnets.*	⬇ spoofed UDP attacks p11: "We also noticed a **decline in UDP-based spoofing attacks** as servers are slowly being secured throughout the internet and are consequently used less frequently for such attacks."	p5: "There was a **dramatic reduction in DDoS activity within our network during the final months of the year.** " p5: "... there was a noticeable trend towards larger (bps) attacks targeting our customers at the end of the year. " Reduction of NTP, increase of memcached, TCP SYN.	p9: Avg duration ⬆3% (11min). Avg attack size ⬆10% (11 Gbps) ⬆81% (6 Mpps). Most attacks were small. 50% of attacks last 5-10min. p10: "When looking at the overall size distribution of attacks in our backbone, we see that while there has been an increase in the number of large attacks, the vast majority of attacks are still small. ... We saw the biggest increase in the 5-20 & 20-50 Gbps attack ranges."	p6: Peak attack bandwidth ⬆19%. p8: Peak attack 813 Gbps, 854 Mpps	p15: "CB attacks have become increasingly less effective, more sporadic. "	No information about the number of vectors in attacks.	No information about targets, such as Industries, regions or countries affected.	p2: "Operating the world's #1 Internet backbone gives us a unique global perspective on the constantly evolving DDoS threat landscape. Using our own network data... When looking at the overall size distribution of attacks in our backbone..."
Cloudflare	DDoS landscape in Q4 2022. The reports are quarterly, and so most comparisons are QoQ, not YoY. Separates in two classes attacks: HTTP/S DDoS and "network layer" attacks.	DDoS Attack Trends for 2022 Q4	Open/Web	2022 Q4	No information about attack counts	"In Q4, Memcached-based DDoS attacks saw the highest growth — a 1,338% increase QoQ". "In second place, SNMP-based DDoS attacks increased by 709% QoQ."	"In Q4, **SYN floods** remained the attacker's method of choice — in fact, almost half of all network-layer DDoS attacks were SYN floods." "The amount of HTTP DDoS attack traffic still increased by 79% YoY" "Application-layer DDoS attacks: Distribution by quarter... we can see a clear downward trend in attacks each quarter this year." Bar plot shows that **HTTP DDoS attacks decreased** in each quarter: 28%, 27%, 24%, 21%.	*This report separates attacks into two classes: Application layer, and Network layer (which actually includes the transport layer e.g. SYN attacks).* "Network-layer DDoS attacks: Distribution by quarter". Quarters: 21%, 24%, 30%, 26%. It does not indicate if the attacks are D/P or R/A.	No plot or table with longitudinal data for the period considered.	"In Q4, the amount of shorter attacks lasting less than 10 minutes decreased by 76% QoQ, and the amount of longer attacks increased. Most notably, attacks lasting 1-3 hours increased by 349% **QoQ** and the amount of attacks lasting more than three hours increased by 87% **QoQ**. Most of the attacks, over 67% of them, lasted 10-20 minutes."	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	"Source and targets of DDoS attacks". Contains a discussion about countries and industries attacked.	"This report includes insights and trends about the DDoS threat landscape - as observed across Cloudflare's global network."
Comcast	Generic report, includes DDoS landscape in 2022, from p21	2023 Comcast Business Cybersecurity Threat Report	Open/PDF	2022	p22: "The year 2022 saw a slight decline in worldwide DDoS attacks. ... Comcast Business detected a total of 51,915 DDoS attacks." *We observed that the number of DDoS attacks in the Comcast 2021 report was different in orders of magnitude, in the millions. We asked Comcast, which indicated that the discrepancy was "due to a change in methodology", without further details.*	p23: "Vectors Responsible for Generating DDos Traffic". Percentages normalised to total traffic *(similar to Cloudflare)*: DNS R/A 7%, 1% R/A other. p23: "While **amplification attacks continued to play a role, they represented a smaller percentage of attack traffic.**" *With benign 85%, we assume DNS R/A was 7/15 or 46% of attack traffic.*	p23: Out of total traffic, TCP SYN 3%. *With 85% benign traffic, we assume that TCP SYN was 3/15 or 20% of attack traffic.*	p23: "Adversaries did not change their tactics much during 2022. Most attacks still used low-complexity, high-impact flooding techniques. This is validated by NetScout's review of all 9.4 million DDoS attacks they tracked last year, which identified total traffic, UDP, and TCP Sync as the top three vectors used" *There is no link.*	Potential decrease in #attacks in December. p22: plot shows that the number of attacks went up July-Aug-Sept (2.8k, 4.5k, 8k), then decreased Oct-Nov-Dec (5k, 5.1k, 3k).	p22: "Short-burst attacks dominate. ... Once again, the bulk of the attacks were under ten minutes long. The trend of short-burst attacks has continued since the prior year." 0-5m (22%), 6-10m (54%), 1-12h (3%).	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	No information about attacks with carpet-bombing.	p23: "31% of Comcast Business detected attacks in 2022 were multi-vector attacks. 82% of all multi-vectors contained DNS amplification vectors."	p23: "Figure 13: DDoS attacks by industry segment detected by Comcast Business in 2022"	No information about sources or methodology used.
Corero	DDoS landscape in 2022	2023 DDoS Threat Intelligence Report	Open/PDF	2022	No information about attack counts	No information about reflection/amplification attacks.	p13: "Data compiled by the Corero Threat Intelligence team and shown in figure 8 confirms a significant 70% increase in the percentage of successfully detected and mitigated DDoS attacks using TCP-based vectors." In the figure, TCP represented 28-38% of attacks when compared to UDP. *Note that unlike TCP, UDP is used in both D/P and R/A attacks, so it is not possible to say what was the increment in D/P.*	p12: ⬆600% in IPv6 traffic	No plot or table with longitudinal data for the period considered.	p18: 75% attacks < 10min, ⬆60% attacks > 60min	p18: 98% attacks < 10 Gbps, ⬆25% high packet rate attacks	p6: ⬆300% CB. 1844 attacks in 2021, 7581 in 2022. p6: "Carpet bomb attacks are difficult to defend against, stymying many of the traditional detect-and-redirect DDoS mitigation techniques." *The report contains a long explanation of CB attacks, including an example (Section 2).*	No information about the number of vectors in attacks.	p14: 29% destination port 53, 17% destination port 80, 7% 123 (NTP). p14: "It is not possible to pinpoint the precise reason for the choice of these destination ports. But, based upon a mapping of the target ports on the intended victim IP/system, our analysis suggests that it is not primarily to attack these specific DNS, web, or NTP-based services. Instead, we believe that these ports are chosen for the access they provide for malicious traffic to enter the network via open ACL/firewall rules."	No information about sources or methodology used.
DDoS-Guard	DDoS landscape in 2022 (Russian)	DDoS Attack Trends in 2022	Open/Web	2022	"1,255,573 is the total number of DDoS attacks detected and successfully mitigated by DDoS-Guard in 2022." "We observe the greatest upsurge in DDoS attacks in recorded history. Ongoing geopolitical events made the number of attacks on Russian websites increase by 700%, compared to 2021."	No information about reflection/amplification attacks.	No specific information about direct/path attacks and associated vectors.	"Emphasis on Application Layer Attacks. We observed an over 600% increase in the number of DDoS attacks in the first half of 2022. Most of them were application layer attacks (L7, according to the OSI model). "	No plot or table with longitudinal data for the period considered.	"The duration of DDoS attacks has decreased, in comparison to 2021. Nevertheless, the frequency has increased by 3-4 times." "In 2022, the vast majority of DDoS attacks lasted up to 20 minutes, and a significant number of them lasted from 20 minutes to 1 hour. Attacks lasting 24 hours or longer comprise less than 1% of the total number of incidents." 700k attacks < 20min, 281k 20min-1h, 178k, 1-6h, 26k 6-12h... 3k > 24h	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	"The primary targets were websites related to the media, government, and financial services." "The number of DDoS attacks on media portals increased by a record-breaking 76 times (51,842 incidents compared to 670 in 2021). Government-related websites were also constantly under attack, with the number of incidents increased by 55 times (20,766 compared to 370). The websites of banks and financial organizations were attacked 20 times more often than in 2021 (27,600 incidents compared to 1,318)."	No information about sources or methodology used.
DDoS-Guard	DDoS landscape in 2022 (Russian). Infographic with a summary of numbers.	Analytical Report on DDoS Attacks for 2022	Open/PDF	2022	p4: 1.25M attacks, compared to 147k in 2021. *The one order of magnitude increase may be associated with the Russia-Ukraine conflict, as this is a Russian provider.* Highest number of attacks in March.	No information about reflection/amplification attacks.	No specific information about direct/path attacks and associated vectors.	*This report separates attacks into two classes: Layer 7, and Layer 3-4.* p2: 171k L3-L4 attacks vs 1M L7 attacks. *This contradicts the reports that state that flooding attacks are the most common, by far.*	p3: Plot shows the number of attacks per month. *There is a visible reduction in November and December 2022.*	p4: "In 2022, we detected a new internal record: the longest DDoS attack lasted 68 days, compared to 52 days in 2021. Though, the overall trend has been as follows: short-duration attacks have become more common, with the total number increasing by 700%."	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	p2: "Distribution of Attacks by Industry"	No information about sources or methodology used.
F5	DDoS landscape in 2022	2023 DDoS Attack Trends	Open/Web	2020-2022	"Overall observed events are down by -9.7%" Figure 2: 984 attacks in 2022, ~1100 in 2021.	No information about reflection/amplification attacks.	"In 2022, Application vector attacks grew dramatically, by 165%, even as the overall number of attacks went down." Of L7-attacks, 93.4% were **DNS request floods**, not DNS R/A; see Terms Used in This Report.	*This report separates attacks into the following classes: Volumetric, Protocol, Application, and Multiple Vector.* "Figure 2 2020-2022 DDoS Attack Category counts. This shows a large increase in the number of Application attacks, with a corresponding reduction in Volumetric and Multiple Vector categories" From plot, Total 984 attacks: Multi-vector (369), L7 (351), vol. (168), protocol (96).	See Figure 10 Peak bandwidth over time 2020-2022. *We see no visible effect.*	No information about attack duration.	"In 2022, the maximum peak bandwidth we observed was 800mbps, down from 1.39tbps the year before, a 42.4% decrease (Figure 3)"	No information about attacks with carpet-bombing.	Fig. 2: 369/984 attacks multi-vector	DDoS attacks targeting DNS ports or services	"A Note on the Analysis... There are, however, a few things to keep in mind when reading any analysis of DDoS trends and events. Bringing a critical frame of mind to any data to determine relevance to your specific situation is key to being able to turn observations into action. **Any dataset relating to DDoS traffic will only show what the collection point was able to observe, and this will be only a fraction of the total DDoS that occurred across the internet.**"

Summary of DDoS Industry Reports 2022

VENDOR	SUMMARY	TITLE	FORMAT	PERIOD	ATTACK COUNTS	R/A	D/P	VECTORS	CHANGES END OF 2022	ATTACK DURATION/SIZE	ATTACK INTENSITY	CARPET BOMBING/PREFIX	MULTI-VECTOR	TARGET	VANTAGE POINTS/SOURCES
Huawei	DDoS landscape in 2022	Global DDoS Attack Status and Trend Analysis in 2022	Open/PDF	2022	p16: "In 2022, Huawei detected 104,922 attacks exceeding 100 Gbps, with an average of 287 attacks per day. The number of attacks at over 100 Gbps is 1.5 times that of 2021 and 2.1 times that of 2020." *With this analysis, the report removes the large number of attacks that are too small to be disruptive.*	No information about reflection/amplification attacks.	p2, p14: "The largest application-layer attack in the Internet history occurred in June 2022, peaked at 46 million rps"	p3: "In the past three years, the proportions of ACK flood and UDP flood attacks in network-layer attacks have been increasing year by year." p19: "In 2022, SYN flood, ACK flood, UDP flood, UDP reflection, and TCP reflection attacks are top 5 network-layer attacks." *Therefore, the fraction of D/P attacks (the three first) is likely higher than that of R/A (the two others).* p19: "In 2022, ACK flood attacks accounted for 23.16%, 2.1 times that in 2021 and 10.9 times that in 2020. The **main reason why the number of ACK flood attacks increases** rapidly is that network-layer CC attacks launched by the Mirai botnet are destructive, and hard to be defended against." *The reason mentioned was the increase of botnets, not a reduction in spoofing, though these may be inter-related.*	p15-18: Plots by month 2020-2022 show some changes in the period Oct-Dec 2022. *However, it is hard to see a meaningful trend.*	p3: "57.40% of network-layer attacks and 40.49% of application-layer attacks last for ≤ 5 minutes"	p2: "There were 232 attacks above 800 Gbps, 1.67 times that in 2021." p2: "In November, China Telecom's security team detected the attack with the annual maximum bandwidth, which peaked at 3.189 Tbps." p2: "In April, China Telecom's security team detected the attack with the annual highest packet rate, which peaked at 861 Mpps."	p14: "The scale of carpet-bombing attacks rapidly increases, with the attacked class C IP address segments surging from 100+ in 2021 to 600+ in 2022. Ultra large-scale attacks pose severe challenges to defense costs."	p21: "In 2022, the proportion of multi-vector attacks accounted for 63.47%, which is less than that in 2021." The bottom plot on the same page shows that in 2022 36% of attacks used 1 vector, while 30% had 5+ vectors. p6: "During the 2022 World Cup, DDoS attacks were extremely active. Multiple attacks on payment platforms and APIs occurred in China. … The entire attack process can be divided into seven phases, and a total of 14 attack vectors were used: UDP flood, spoofed QUIC flood, SYN flood, large SYN flood, SYN flood with real source IP addresses, network-layer CC, NTP reflection, SSDP reflection, DNS reflection, UDP fragment, TCP reflection, ICMP flood, other flood, and application-layer CC (HTTP flood)."	p39: "API calls currently account for more than 83% of all Internet traffic according to Akamai. Cloudflare claims that 56% of traffic traversing its network is related to APIs. Due to the large quantity of APIs and enterprises' inadequate attention to API security, API attacks have become one of the biggest threats faced by enterprises. Cloudflare also claims that its network security devices block more traffic attacking APIs than that attacking websites. **This indicates that APIs have become the main target of network attacks.**" p39: "Attack Type Distribution. By tracing the DDoS attacks targeting APIs, we find that APIs suffer most of the attacks that have occurred on the Internet. In 2022, the top 5 types of attacks targeting APIs were network-layer CC, SYN flood, UDP flood, HTTP flood, and UDP reflection attacks." *Note: CC = Challenge Collapsar. CC attacks are mainly used to attack web pages (via invalid requests).* p39-49: Attacks against APIs. p51-72: Attacks against the finance industry.	p77: "The data involved in this report originates from China Telecom Cybersecurity Technology Co.,Ltd., China Unicom Digital Technology Company Limited, Baidu Security, Nexusguard, Huawei Cloud, and DDoS attack related data from Huawei's customers after authorization."
Imperva	DDoS landscape in 2022	DDoS Threat Landscape Report 2023	Form/PDF	2021-2022	p9: "Application Layer DDoS attacks increasing year on year. The number of application layer DDoS attacks has been on an upward trajectory year on year as the chart below shows." *The Y axis does not show values or units, so it is not possible to read the magnitude of the growth, even in relative terms. The same problem applies to other plots on the same page.* *The report does not comment about the global number of DDoS attacks, considering all categories.*	No information about reflection/amplification attacks.	p8: "Application Layer (L7) DDoS attacks increased by a staggering 82% YoY in 2022 vs 2021." SYN 21%	*This report separates attacks in two classes, Application Layer DDoS Attacks, and Network Layer DDoS Attacks, and presents results separately.* p12: "Network Layer DDoS most common attack vectors." According to the pie chart on the same page: UDP 42%, SYN 21%, TCP 11%, DNS response 7.8%, NTP 7.7%.	p8: The bar plot shows monthly Application Layer DDoS attacks. *There is some growth in the last three months of 2022.*	p10: "Application Layer DDoS Attack Duration. Our research shows that Layer 7 DDoS attack duration is becoming longer in duration with **almost 40% of all Layer 7 DDoS attacks lasting more than 12 hours**, an increase of 33% of attacks in 2021." p13: "Network Layer DDoS attack duration. **66%** of all Network Layer DDoS attacks mitigated by Imperva lasted **15 minutes or less** in 2022." p10, p13: pie charts. L7 attacks longer (40%>12h, 27%<15m) than L3/L4 (66%<15m, 12-24h 1.2%).	p3: "The largest Layer 3 and 4 DDoS attack occurred in July and peaked at 1373 gigabits per second (Gbps). Layer 3 and 4 attacks rose dramatically in August 2022 in comparison to any other month of the year." p11: "The largest protocol attack mitigated peaked at 591 million packets per second (Pps)."	No information about attacks with carpet-bombing.	p11: "In 2022, **almost 73% of all layer 3 and 4 DDoS attacks consisted of a single vector** which is in sharp contrast to 2021 when only 21% of attacks were single-vector. This might indicate that DDoS attackers are leveraging single vector attacks as part of a wider attack strategy possibly as a distraction tactic."	p9: "Application Layer DDoS attacks growth by industry. Application Layer DDoS attacks on the Telecoms and Internet Services Provider (ISP) sector increased by 250% in 2022 vs 2021. Application Layer DDoS attacks on Financial Services more than doubled in 2022 compared to the previous year's increase by 121%." p12: "Network Layer DDoS most targeted industries. Financial Services and Banking targets accounted for around 16% of all network layer DDoS attacks in 2022 followed by the Entertainment industry at 8.4%." p6: "Why APIs are a Target for DDoS Attacks. A shift to more modern applications has meant an explosion in the adoption of API endpoints which, as they become more intrinsic to a company's infrastructure, present new opportunities for cybercriminals to cause disruption." *Similar to Huawei's report, there is some emphasis on attacks against APIs.* p5: "No one is safe from DDoS. In December 2022, it was reported that a DDoS strike on the Vatican website took it offline for several days, possibly the work of Russian activists."	p3: "The report leverages intelligence provided by Imperva Threat Research based on data from application and network DDoS attacks we have mitigated. It also provides additional observations based on general DDoS activity throughout the year."
Kapersky	DDoS landscape in Q3 2022. *Report highlights threat actors and high-profile attacks, but does not describe them. It includes relative/normalised trends and stats.*	DDoS attacks in Q3 2022	Open/Web	2022 Q3. *No 2022 Q4 report.*	"The number of DDoS attacks in Q3 2022 fell again. Having decreased by 13.72 percent in the previous reporting period relative to the one before, this quarter it dropped by a further 27.29 percent, to 57,116." Figure: "Comparative number of DDoS attacks, Q32021,Q2 and Q3 2022.Q3 2021data is taken as100%. The first thing worth noting is the significant rise in the number of DDoS attacks of all types relative to the previous reporting period." The attack count in Q3 2022 is 203.66% compared to Q3 2021.	No information about reflection/amplification attacks.	"The share of UDP flood fell from 62.53 to 51.84 percent, but remained the most common type of DDoS. The second most common, SYN flood, on the contrary, increased its share to 26.96 percent. TCP flood (15.73%) reversed its decline, adding more than 4 percentage points to hold on to third place. GRE flood and HTTP flood made up 3.70 and 1.77 percent, respectively, of the total number of attacks." "UDP flood accounted for 51.84 percent of the total number of attacks, and SYN flood for 26.96 percent."	"In Q3 2022, the ranking of DDoS attack types was unchanged from the previous reporting period." "Moreover, DDoS attacks on HTTP(S) this quarter exceeded those on TCP for the first time, despite the latter being easier to organize and still the most common type of DDoS." "What's most interesting is that, in absolute terms, the **number of attacks on HTTP(S) has remained quite stable over the past year**. The **share of attacks on TCP is on a downward curve**, which reflects well the general trend: the share of dumb DDoS attacks is falling, while that of smart attacks is growing."	No plot or table with longitudinal data for the period considered.	"Attacks lasting less than four hours accounted for 60.65 percent of the total duration of attacks and for 94.29 percent of the total number of attacks." "In Q3 2022, sustained attacks of 20 hours or more accounted for 19.05 percent of the total duration of attacks." In Q3, 19% of attacks > 20h; 3.16% of attacks 3.16% 5-9 hours.	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	"The number of unique targets of DDoS attacks in this report is counted by the number of unique IP addresses in the quarterly statistics." *Carpet bombing attacks would count as many different targets.*	No information about the number of vectors in attacks.	"A total of 39.61 percent of targets, affected by 39.60 percent of attacks, were located in the US." "In Q3 2022, the top four countries in terms of resources attacked remained unchanged from the previous reporting period. The US (39.60%) remained in first place, despite losing 6.35 percentage points. Mainland China's share (13.98%) increased by almost the same amount, up 6.31 percentage points, securing second place. Germany (5.07%) remains in third and France (4.81%) in fourth place."	"DDoS Intelligence statistics are limited to botnets detected and analyzed by Kaspersky. "
LINK11	DDoS landscape in 2022	DDOS-REPORT 2022	Form/PDF	2022	p8: "In 2022, the number of attacks dropped by 79% compared to last year"	p19: "In 2022, LSOC recorded a flood of amplification techniques. The Internet service most frequently exploited for attacks and abused as an amplifier in 2022 was DNS (60%), followed by NTP (24%), SNPM (4%), and Apple Remote (4%)." In 2021, DNS was 17%, and NTP, 19%.	No specific information about direct/path attacks and associated vectors.		p15: Figure shows that B/W peak decreased around Oct-Dec 2022.	p13: "The duration of DDoS attacks recorded on the Link11 network in 2022 has shortened compared to the same period last year. While there were significant outliers almost every month, the overall attack duration decreased" p14: "Most attacks (71%) lasted less than 5 minutes. One-fifth of all registered attacks (20%) were between 5 and 15 minutes long, and another 8% were up to 60 minutes long. Only about 1% of attacks were longer than 60 minutes." Longest attack 28h15m. 71% attacks <5min. 20% 5-15 min. 1% >1h.	p15: "largest attack in 2022 was stopped at 574 Gbit/s, which is very low compared to 2021." p15: "While the average number of packets per second was 3.3 million during the review period, the packet rate was significantly lower in 2021." p15: "A look at the correlation between the duration and intensity of DDoS attacks reveals a change, especially for the first half of 2022: the attacks are simultaneously more intense and shorter"	p15: "The reason for this is less "carpet bombing" in the attacks registered on the Link11 network. These technically complex DDoS attacks are difficult to detect because they have very low traffic per IP address"	p18: "The highest number of concurrent vectors observed in the Link11 network was 18, the largest multi-vector attacks observed in Link11's network to date."	No information about targets, such as Industries, regions or countries affected.	No information about sources or methodology used.
Lumen	DDoS landscape in Q4 2022	Lumen Quarterly DDoS Report Q4 2022	Open/PDF	2022	p7: "In Q4 2022, Lumen mitigated 9,195 attacks — more than any other quarter in 2021 or 2022. This is a 66% increase from Q3 and a **147% increase year over year**." *However, it could be an increase of 22%, by comparing with the sum of the numbers in the 4 reports of 2021: 6.1k Q1, 4.5k Q2, 5.5k Q3, 9k Q4.*	p12: "DNS amplification attacks became more popular in the second half of 2022 and in **Q4 account for 29% of activity**, which is a 73% quarterly increase and a drastic spike compared to Q4 2021 when it only accounted for 1% of activity."	p12: "TCP SYN Flooding was still used frequently, accounting for 25% of activity, which was a 16% increase from Q3 and an 89% increase from Q4 2021."	p12: "Static Filtering accounted for 16% of activity in Q4, which is a 4% decrease quarter-over-quarter." *This seems to be the only report to mention static filtering as a class of attack, but it is actually a mitigation form.*	No plot or table with longitudinal data for the period considered.	p10: "68% of all attacks on Lumen On-Demand DDoS mitigation customers in Q4 were under 10 minutes." See plots on the same page.	p8: "In the first half of the year, Lumen mitigated several large attacks, including 775 Gbps in Q1 and 1.06 Tbps in Q2. However, the median attack size at those times were rather small (0.19 Mbps and .11 Mbps respectively)." According to table, in 2022, largest attack was 20% smaller (bps) than 2021.	No information about attacks with carpet-bombing.	p13: "We finished out the year with DNS amplification combined with TCP SYN Flooding being the most leveraged multi-vector attack".	p14: "Of the 1,000 largest attacks Lumen mitigated, 97% targeted these top five verticals (in order): Telecommunications, Software and Technology, Gaming, Government, and Hosting. … It is important to note that a single government customer represented 60% of all the attacks Lumen mitigated in Q4"	p5: "Where does this threat intelligence come from? This report is developed with the participation of a few teams — our DDoS mitigation operations team and our Black Lotus Labs® team work together to come up with insights for our readers. Black Lotus Labs is the threat intelligence team within Lumen. It is made up of a group of security professionals and data scientists whose mission is to leverage Lumen's global network visibility to both help protect our customers and keep the internet clean. Black Lotus Labs uses threat hunting and analysis, as well as machine learning and automated threat validation, to identify and disrupt the work of malicious actors."
Microsoft	DDoS landscape in 2022	2022 in review: DDoS attack trends and insights	Open/Web	2022	"In total, we mitigated upwards of 520,000 unique attacks against our global infrastructure during 2022."	In Figure 2. Attack type, UDP R/A 9%. "We observed **TCP reflected amplification attacks** becoming more prevalent, with attacks on Azure resources using diverse types of reflectors and attack vectors. This new attack vector is taking advantage of **improper TCP stack implementation in middleboxes**, such as firewalls and deep packet inspection devices, to **elicit amplified responses that can reach infinite amplification in some cases**. As an example, in April 2022, we monitored a reflected amplified SYN+ACK attack on an Azure resource in Asia. The attack reached 30 million packets per second (pps) and lasted 15 seconds. Attack throughput was not very high, however there were 900 reflectors involved, each with retransmissions, resulting in high pps rate that can bring down the host and other network infrastructure."	"TCP attacks remain the most common attack vector. TCP attacks were the most frequent form of DDoS attack encountered in 2022, **comprising 63% of all attack traffic**, which includes all TCP attack vectors: TCP SYN, TCP ACK, TCP floods, etc." *The analysis seems to use traffic to rank the prevalence of attacks, not attack count; this would potentially highlight volumetric attacks.* In Figure 2. Attack type, UDP flood 13%. "Out of UDP flood attacks, spoofed floods consumed most of the attack volume with 53%." "Packet anomaly attacks made up 15% of attacks." *It is unclear what kind of packet anomaly the report refers to, but we assume this is invalid headers, such as a TCP packet with no bits on.*	UDP 22% of attacks.	Figure 1. Attack volume shows how the attack volume varies daily throughout the year. Apart from the very end, the volume stays **above the average for most of the last quarter**.	"Shorter attacks continue to be popular. Shorter duration attacks were more commonly observed this past year, with 89% of attacks lasting less than one hour. Attacks spanning **one to two minutes made up 26%** of the attacks seen this year. Attackers often use multiple short attacks over the span of multiple hours to make the most impact while using the fewest number of resources."	"In May, we mitigated a 3.25 terabits per second (TBps) attack in Azure, the largest attack in 2022."	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	"US, India, and East Asia top regions targeted by attacks" USA represents 45% of attacks, and India, 13%.	No information about sources or methodology used.
NBIP	DDoS landscape in Q4 2022	DDoS attack figures from the fourth quarter 2022	Open/PDF	2022 Q4	379 attacks in Q4 2022. Bar plot attacks/quarter: 666, 514, 442, 379.	19.6% DNS amplification; 24% NTP amplification; 4.7% LDAP amplification. *By comparing the quarterly reports in 2022, we observe that these fractions fluctuate substantially. For example, in Q2, there was 41% of DNS amplification, and Memcached was present with 8%.*	Pie chart shows 21.5% TCP flag; 10.3% UDP flood.		"A **consistent decline in the number of DDoS attacks quarter over quarter**, with this trend continuing since the fourth quarter of 2021."	"Prolonged attacks >4 hours" 38 in Q4	"Significant DDoS attacks, with large attack sizes (381 Gbps and 364 Mpps)."	No information about attacks with carpet-bombing.	"The use of multi-vector attacks is on the rise, with an increasing number of attackers attempting to simultaneously overwhelm their victims' networks by utilizing a diverse set of attack methods."	"Geopolitically, the ongoing conflict in Ukraine has led to an increase in targeted DDoS attacks on government services and critical infrastructure. This trend is expected to continue in 2023, with an emphasis on attacks on the financial, energy, and healthcare sectors."	No information about sources or methodology used.

Summary of DDoS Industry Reports 2022

VENDOR	SUMMARY	TITLE	FORMAT	PERIOD	ATTACK COUNTS	R/A	D/P	VECTORS	CHANGES END OF 2022	ATTACK DURATION/SIZE	ATTACK INTENSITY	CARPET BOMBING/PREFIX	MULTI-VECTOR	TARGET	VANTAGE POINTS/SOURCES
NetScout	DDoS landscape in 2H 2022	5th Anniversary DDoS Threat Intelligence Report: Unveiling the New Threat Landcape	Open/PDF	2022 2H	p3: "DDoS attacks nearly reached a plateau of 13 million for 2022"	p9: "Direct-Path DDoS Attacks. ... **reflection/amplification attacks declined 18 percent since 2020**" p9: Figure 10: Top 5 Vectors. 1,189,774 DNS amplification, 1,108,008 TCP SYN/ACK Amp	p3: "It was in early 2021 when we detected a **tectonic shift in preference by adversaries to TCP-based, direct-path attacks**—a move that carries throughout 2022 and one that organizations and enterprises must address to protect stateful devices and downstream customers." p9: "Direct-Path DDoS Attacks. ... While reflection/amplification attacks declined 18 percent since 2020, **direct-path attacks climbed 18 percent over three years**, creating a difference of nearly 2 million attacks between them (Figure 12)." p9. "HTTP and HTTPS Application-Layer Attacks. ... Based on a sampling of our data set, we witnessed a **487 percent increase in HTTP/HTTPS attacks since 2019** (Figure 11)." p9: Figure 10: 1,979,785 TCP ACK, 1,349,140 TCP SYN, 1,092,525 TCP RST p9. "A form of application-layer attack, DNS query floods have more than tripled since they really became weaponized in 2019, a 243 percent increase in adoption of this attack technique (Figure 14). The average daily attack count for 2022 is approximately 850 attacks, a 67 percent increase over the 522 average in 2021."		p9: Figure 12: Reflection/Amplification vs. Direct-Path Attacks. *Shows a split between the amount of Reflection/Amplification attacks and Direct-Path attacks in early 2022, with the Direct-Path being higher.*	p3: "Figure 1: Attack Duration Breakdown (2019–2022)": 25%<5min, 36% 5-10min, 30% 10-60min, 7% 1-12h	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	p10: "This trend started in November 2021 and really accelerated in August 2022. Daily attacks using this method rose from an average of 670 in 2021 to an average of 1,134 in 2022, a **69 percent increase.**" Figure 13: Carpet-Bombing Attacks show the daily attack count.	p3: Figure 2: Multi-vector breakdown. **60% 1 vector, 29% 2-5 vectors**, 8% 6-10 vectors, 3% 11+ vectors	p12: DDoS Attack Motivations	p3: "More than two decades of working with **more than 500 internet service providers** (ISPs) has allowed us to build a sensor network that spans more than 50 percent of the world's largest networks." p5: "Global visibility is key to assessing the DDoS threat landscape. Without visibility, it would be extremely difficult to create a timeline of history, identify trends, and adequately prepare for and defend against network-based attacks such as DDoS. Our global sensor network gives NETSCOUT incredible visibility into the networks around the world, allowing us to see a staggering 401+ Tbps average of internet traffic (Figure 3)—an estimated 50 percent of international transit capacity. That is 3 petabytes or 24.06 petabits of transit per minute!" p7: "Enterprise. With 13 million attacks in the ISP networks, **we turned our attention to the enterprise**, where we gathered data from **one-fifth** of our enterprise customers and found more than 3,500 events per day or 145 per hour. These events stemmed from **high-impact traffic tripping predefined thresholds, creating a denial-of-service (DoS) alert. Not all of these alerts are DDoS attacks;** high-throughput scanning also can trip these thresholds. Nonetheless, these events along with GeoIP blocks, application-layer attacks, and inbound brute-forcing/ exploitation resulted in traffic being dropped to downstream users on these networks."
NexusGuard	DDoS landscape in 2022	DDoS Statistical Report for 2022	Form/PDF	2022	p3: "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."	p4: "**↑2,472.03%** NTP Amplification Attack". p6: "**↑28,233.16%** Memcached Attack". *These values are too high; we are not confident they are correct.* p4: Figure 2 - Top 10 Attack Vectors in 2021 and 2022. for the prevalence of attack vectors. NTP 31%, Memcached 14%, DNS Amp 2.34%, p7: "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%." p9: "Volumetric (Amplification) attacks, **contributing 51.28% of the total attacks** recorded in 2022, **increased by 414.63% YoY**"	p6: "**↓**0.23% D/P volumetric flood" p6: "**↑**718% Application attacks"	p7: Types of Attack Vectors. Figure 2	No plot or table with longitudinal data for the period considered.	p13: "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."	p14: "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.88.14% <1 Gbps. **0.18% >=10 Gbps.**" See Fig. 8.	p15: "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." *We believe this description is equivalent to a carpet-bombing attack.* According to Summary 1 - Bit-and-Piece Attacks in 2021 and 2022, Targeted ASNs 240 Total No. of IP Prefixes (Class C) Under Attack 3,079	p11: "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." p12: "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%."	p23: Reflected Attack Destination Distribution.	p26: "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."
Nokia	General security report that includes some DDoS from p16. Not much information	Threat Intelligence Report 2023	Form/PDF	2021-2023	No information about attack counts	No information about reflection/amplification attacks.	No specific information about direct/path attacks and associated vectors.		*Based on Fig. 9, it looks like there were fewer attacks from Sept 2022 til March 2023 than in the preceding 6 months.*	No information about attack duration.	p16: "Figure 9. Distribution of DDoS attacks by peak intensity (Gbps), January 2022 – March 2023" *There is no explanation of the figure, but we believe there are ~7-8 attacks at the Tbps level.*	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	Comments about DDoS being used in cyberwarfare.	Nokia Deepfield
NSFocus	DDoS landscape in 2022	2022 Global DDoS Attack Landscape Report	Form/PDF	2022	p1: "DDoS Attacks Increased **Dramatically**. The data shows that DDoS attacks in 2022 **increased by 273%** compared to 2021" p6: "As a popular attack method in the past two years, TCP reflection attacks represented 3%"	p0: "About one-third of terabit attacks were reflective UDP attacks, while the rest were mainly non-reflective UDP attacks." p6: "As a popular attack method in the past two years, TCP reflection attacks represented 3%"	p7: "UDP Fragment Flood Stood Out. In 2022, UDP flood attacks, SYN flood attacks, and UDP fragment flood attacks were top 3 network-layer DDoS attacks."	p6: Three pizza plots show vector prevalence, but without actual numbers.	*Multiple plots show values month-by-month. No discernible effect at the end of the year. On the contrary, high-volume attacks increase in Oct-Nov-Dec.*	p8: "Nearly 70% of global DDoS attacks were shorter than 10 minutes, about 20% lasted 10 to 30 minutes, and the rest exceeded 30 minutes. Currently, "quick spike" attacks prevail." ~70% of attacks <10m, ~20% 10-30m.	p1: "High-Volume DDoS Attacks Were on the Rise. In 2022, the number of terabit-level DDoS attacks was approximately 40, and the attack peak exceeded 1 Tbps in six months" p2: "On average, an attack exceeding 100 Gbps happened every hour."	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	p5: "DDoS Attacks Increasingly Targeted Critical Infrastructure" p4: "DDoS attacks against a single target became increasingly persistent. 56.91% of victims experienced only one DDoS attack in 2021, whereas victims were more prone to multiple DDoS attacks once identified as the target in 2022."	No information about sources or methodology used.
Qrator	Quarterly report about DDoS and BGP incidents. DDoS landscape in 2022 Q4. *Report distingues between L3-L4 and L7 attacks.*	Q4 2022 DDoS attacks and BGP incidents	Open/Web	2022 Q4	"In 2022, DDoS attacks increased by 73.09% compared to 2021."	"Amplificators and Amplification factors in 2022. The data is for 2022 - the number of amplificators/reflectors publicly available on the internet and the average amplification factors we've registered." *Presents the number of exploitable servers and the corresponding amplification factor, but does not provide information about such attacks.*	"In the fourth quarter of 2022, the following attack vectors were prevalent: UDP flood, accounting for 37.05% of all L3-L4 attacks; SYN flood, responsible for 26.84% of volumetric attacks; and IP flood, with a smaller share of 13.8%." "**UDP flood prevailed as the leading attack vector throughout the year**, except for the first quarter of the year, when the SYN Flood was the top technique." "In the attack vector statistics without concurrency, we again see the prevalence of the UDP flood, although the proportion is lower than in Q3 when it was 51.79%. The SYN flood has gained the most, rising from 20.37% in Q3 to 41.34% in Q4." *We note that the numbers presented in the report do not include any form of reflection-amplification.* "Application Layer Attack Distribution. Unlike Q3, the largest category in Q4 2022 is **Request Rate Patterns**, which includes anything that deviates from what is expected from a legitimate user in terms of request rate, and collected **30.37% of Q4 2022 application layer attacks**. It is followed by Rotating Client Secondary Attributes, which refers to an **unusual set of headers in the request**, and accounts for more than a quarter - **28.05%** - of L7 DDoS attacks. That differs from the third category, **Abnormal URL Traversal**, which is exactly what it sounds like - an action that a legitimate user often wouldn't even be able to perform, where we saw **11.77%** of the attack data. **Broken HTTP semantics now accounts for "only" 6.88% of L7 attacks**. The top four categories together account for 77.07% of L7 attacks, with 13.10% in Multiple Matched Criteria, where we put all concurrent L7 attacks.	The diagram "Attack Vectors Concurrency" shows a detailed breakdown of vectors. *This is more accurate than similar plots in other reports since it represents both isolated and concurrent use of vectors.* "As we mentioned earlier, the interchange between IP (fragments) flood and UDP flood quarter over quarter is somewhat highly expected. Additionally, we expect this trend to stay in the future. The reason is attackers are trying to improve the overall efficiency of their devices by choosing larger amplification targets (like DNS records), and it is pretty standard that those chunks of data significantly surpass the MTU limit. Thus fragmentation is inevitable." *The example indicates that large DNS responses, likely from amplification, can be reported as IP fragmentation.* "The top-3 vectors combined make 77.69% of all the mitigated attacks"	Diagram "Record year in DDoS attacks" shows side-by-side the L3-L4 and L7 attack fractions per quarter. *We see that L3-L4 attacks were much smaller in Q4 (13.11%) than other quarters (43.20%, 23.20%, 20.50%). The same reduction in Q4 was not visible in the L7 numbers (quarter fractions were 21.44%, 42.19%, 15.10%, 21.27%).*	"Comparing the duration data QoQ, the average attack time has almost doubled - from 1510 seconds in Q3 2022 to 2503 seconds in Q4. However, the median duration decreased for the first time since Q2 2022, from 390 seconds to 210 seconds." "But the longest attack in Q4 lasted for 250,500 seconds - **more than 69 hours**, which is still less than what we've seen during Q2 2022 when one of the attacks lasted **more than 100 hours**, and especially Q1, when one attack lasted for **almost 11 days**."	"On the bandwidth side of the attacks, we see that UDP flood and TCP flood are closer at the maximums - **621.86 Gbps and 480.8 Gbps** respectively. However, the difference is much more significant in the median, where the UDP flood shows 1.79 Gbps, which is still more than two times lower than the IP flood median bandwidth of 3.71 Gbps." "In Q4 2022, the **average attack bandwidth was 9.736 Gbps** - the record average bandwidth in 2022. These values only apply to volumetric attacks."	No information about attacks with carpet-bombing.	Diagram provides numbers about the concurrent use of vectors, i.e. multi-vector attacks. *It should be possible to estimate the fraction of multi-vector attacks from these numbers.*	No information about targets, such as Industries, regions or countries affected.	No information about sources or methodology used.
Radware	DDoS landscape in 2022	2022-2023 Global Threat Analysis Report	Form/PDF	2022	p5: "The total number of malicious events blocked by Radware's Cloud DDoS Service in 2022 grew by 233%, compared to 2021. The number of DDoS attacks grew by 150%." p5: "Throughout the year, the number of DDoS attacks per customer kept increasing every quarter, from less than 1,000 attacks **per quarter in Q4** of 2021 to over 2,500 attacks **per customer in Q4** of 2022. By the end of 2022, the average number of attacks mitigated per customer increased by over three times." p5: "the number of attacks a customer witnessed per day at the end of 2021 was 8.41, compared to 29.3 attacks on average per day by the end of 2022, a 3.5x increase."	p15: "DNS amplification was the amplification attack vector that generated the most volume in 2022, representing 77.1% of the total amplification volume. NTP amplification was the second most abused amplification attack vector, accounting for 13% of the volume."	p14: "By a significant margin, **the top attack vector was UDP flood (78.1%)**, followed by UDP fragment flood (5.73%). TCP attacks through several variations of flag attacks completed the vectors above 1% comprising TCP SYN (5.53%), TCP Out-of-State (5.27%), TCP SYN-ACK (2.27%) and TCP RST (1.59%) floods." *Based on another information in the report, it is 78.1% of packets.*		p5: Fig. 2: There was no visible reduction in the last quarter.	p6: Figure 6: Average attack duration per attack size	p6: Fig. 4: substantial increase in the number of smallest (rate < 1 Gbps), modest increase of largest (rate > 250 Gbps) attacks. reduction in all other rates p8: "The largest attack recorded in 2022 was 1.46Tbps, 2.8 times compared to the largest attack of 520Gbps in 2021." *In the Americas and globally.*	No information about attacks with carpet-bombing.	p21: "Figure 40: Number of dissimilar attack vectors per attack as a function of attack size". Attacks > 100Gbps had ~9 vectors.	p7: "Regions and Industries. Finance was the most attacked industry in 2022, with 52.6% of the overall attack activity and a frequency of attacks growing 2.4% compared to 2021"	No information about sources or methodology used.
Zayo	DDoS landscape in **2023 1H**. Zayo is a tier-1 ISP.	Protecting Your Business From Cyber Attacks: The State of DDoS Attacks DDoS (Insights From Q1 & Q2, 2023)	Open/PDF	2023 1H	p6: From bar plot, number of attacks in 2022 1H is approximately 19k (and ~72k attacks in 2023 1H)	No specific information about the use of reflection or amplification.	No specific information about direct/path attacks and associated vectors.		No plot or table with longitudinal data for the period considered.	p11: "The Duration of DDoS Attacks Attacks are getting longer, but **over 83% of all attacks are still short-burst, lasting 10 minutes or less**." p11: "The longest attack in Q2 was 42 days" p13: "Duration of Attacks by Industry Q1 and Q2, 2023" Plot shows that attacks against the Government sector are much longer.	No information about attack intensity, i.e. peak bandwidth or packet rate of attacks.	No information about attacks with carpet-bombing.	No information about the number of vectors in attacks.	p9: "Total Number of Attacks Per Industry QoQ." Plot shows the number of attacks per industry, with Telecom being much higher than the rest. p10: "In both Q1 and Q2, telecommunications companies consistently experienced more DDoS attacks than any other industry. And from Q1 to Q2, this industry's attack activity grew a staggering 1,175%."	p5: "This report reviews DDoS attack data collected from Zayo's network-based DDoS Protected customers."

Summary of DDoS Industry Reports 2022

VENDOR	SUMMARY	TITLE	FORMAT	PERIOD	ATTACK COUNTS	R/A	D/P	VECTORS	CHANGES END OF 2022	ATTACK DURATION/SIZE	ATTACK INTENSITY	CARPET BOMBING/PREFIX	MULTI-VECTOR	TARGET	VANTAGE POINTS/SOURCES
Discussion			*Most (17) reports are open, while 7 require completing a form. Most (16) reports are PDFs, while the remaining 8 are Websites.*	*Most (15) reports are said to be yearly, usually covering 2022, and comparing with 2021 or earlier. Not all yearly reports have been released regularly. Four reports are issued quarterly.*	*10 reports indicated growth in the total number of attacks over the previous year (or years, as in Netscout case). 3 reports did not include a comparison, and 5 did not provide attack counts. 4 reports indicated a reduction in attacks.*	*We could not find information about R/A attacks in 8 reports. While 3 reports indicate a **reduction** in R/A (Arelion, Comcast, and Netscout), 2 reports show an **increase** (Link11 and NexusGuard), with Microsoft reporting an increase of TCP reflection.*	*We could not find any information about D/P attacks or vectors in 5 reports. No report indicated a decrease in D/P attacks. Several reports stated the prevalence of D/P attacks, but did not indicate whether this form of attack increased or decreased compared to the previous year. 5 reports observed an **increase** in either HTTP/S attacks or, more broadly, L7 attacks.*	*Reports varied wildly in how they presented data about attack vectors. There were differences in the name of the vectors and potential overlaps, with occasional ambiguous use of terms. Almost no report clarified how attacks with multiple vectors were counted; the notable exception was Qrator.*	*Generally, information was not present or had to be inferred from graphs showing the variation of some metric through time (weeks, months, quarters, years). The graphical representation of some plots made it hard to read the values. It was often the case that values oscillated wildly from period to period, such as quarter to quarter.*	*Reports generally differed in the set of intervals chosen to group attack durations, making it very hard to compare results among reports. For example, while one report may have used 0-1min, 1-10min, and > 10min, another may have used < 5min, 5-10min, 10-60mn, > 60min.*	*Reports generally differed in the set of intervals chosen to group attack intensity, making it very hard to compare results among reports. For example, while one repot uses < 1 Gbps, 1-100 Gbps, > 100 Gbps, another could have used 0-5 Mbps, 5-1000 Mbps, > 1000 Mbps.*	*Many different terms were used to refer to carpet-bombing. These include "horizontal attacks", "prefix attacks", and "bit-and-piece". Some reports ignore the technique, while others emphasise it, to make the point that attacks are becoming harder to mitigate.*	*While 11 reports completely ignore the issue of multi-vector attacks, some reports highlight it, as a way to emphasise the growing complexity of attacks.*	*In this column, "target" may refer to very different aspects of attacks. We considered analysis of targeted industries and/or regions/countries (potentially linked to geopolitical issues); we did not consider the attack layer or type of service (e.g. DNS). It is possible that reports often highlighted the affected industries to make the business case that they need to pay for protection, and protection needs to be effective against increasingly more powerful and more complex attacks. In 5 reports, there was no information. many cases. The grouping of Industries or sectors (the terms used) varied substantially, and the numbers were very different among reports.*	*Some of the reports state that the data comes from their networks. One (F5) acknowledges explicitly the impact that this may have on the generalization of trends. Generally, reports do not clarify how the data was collected, from which regions of the globe, if from enterprises or ISPs, etc. There are some notable exceptions, such as Netscout. Many reports (A10, Arelion, Lumen, Netscout, and NexusGuard) highlight the need for Internet and attack visibility.*