NEXUSGUARD®

Distributed Denial of Service (DDoS) Trend Report 2024

Table of Contents

Executive Summary

In 2023, the digital landscape faced a transformative wave of Distributed Denial of Service (DDoS) attacks, pushing the boundaries of what is considered a severe threat, with attacks peaking at 700 Gbps and 80 million packets per second. These incidents spanned various industries, from gaming to financial services, highlighting DDoS as a pervasive risk.

Notably, hacktivism has become a key motivator behind these attacks, targeting government and vital services for political ends. This shift towards politicized cyber tactics underscores the growing impact on national security and global diplomacy.

The Nexusguard 2024 Annual DDoS Trend Report offers an insightful analysis, revealing a 54.74% drop in attack frequency but a significant 233.33% rise in average attack size, suggesting a move towards more devastating assaults. The year's largest attack reached 700 Gbps, a 93.42% increase from the previous year, despite a decline in the prevalence of UDP-based, TCP-based, amplification, and application-layer attacks. This comprehensive data is crucial for organizations facing the evolving threat landscape, providing a strategic foundation for enhancing cybersecurity defenses. The report emphasizes the need for preparedness against more sophisticated DDoS attacks, guiding the development of effective protection strategies for the future.

Key Observations for 2023

- In 2023, the total attack count and average attack size decreased by 54.74% and increased 233.33% respectively compared to the figures registered in 2022.
- Compared to 2022, the maximum attack size increased by 93.42%, with the maximum attack size clocking in at 700 Gbps.
- UDP based attacks remained the most predominant type of attack in 2023, decreased by 58.29% YoY. The number of TCP based attacks decreased by 37.20% in the same period a year ago.
- Amplification attacks decreased YoY by 54.94%, while Application attacks decreased by 19.20% YoY.

Key Observations for 2023

Metrics

Total Attacks

vs. 2022

-54.74%▼

Attack Sizes

Maximum

700.00 Gbps

vs. 2022

93.42%▲

Average

0.80 Gbps

vs. 2022

233.33%▲

Top 3 Attack Types

1

NTP Amplification Attack

vs. 2022

-62.58%▼

2

HTTPS Flood

vs. 2022

-19.67%▼

3

DNS Amplification Attack

vs. 2022

165.58%▲

DDoS Attack Category

Volumetric (Amplification)

vs. 2022

-54.94%▼

Application Attack

vs. 2022

-19.20%▼

Volumetric (Direct Flood)

vs. 2022

-68.74%▼

A 5-year trend analysis

Over the span of five years from 2019 to 2023, DDoS attack trends have been influenced by a variety of global events, with correlations between these events and fluctuations in DDoS activity. The surge in attack numbers in January 2023, which outstripped the collective figures from the previous five years, was followed by a notable decrease in March 2023, marking the lowest distribution within that five-year window. The subsequent gradual increase from April to September 2023, and the moderate decline starting from October, can be connected to several key global incidents and developments.

Notably, geopolitical tensions, particularly the Russia-Ukraine war and the NATO expansion bids by countries like Finland and Sweden, have been significant drivers of the rise in DDoS attacks. These events have often been met with cyber retaliation, as evidenced by the targeting of Finland by pro-Russian hacktivists during its NATO bid and a substantial 500 Gbps DDoS attack experienced by Sweden around the time of its own NATO bid.

The increase in attacks against wireless telecommunications providers, with a 79% rise globally in the second half of 2022 and a staggering 294% among APAC providers in the first half of 2023, may correlate with the increased adoption of 5G networks and the subsequent shift in broadband gaming users to 5G fixed wireless access.

Additionally, the escalation of DDoS attacks aligns with the adoption of new technologies and infrastructures, such as 5G networks and the utilization of bespoke infrastructure like bulletproof hosts or proxy networks by adversaries. These methods allow for dynamic and persistent DDoS campaigns, making them more difficult to mitigate.

The rise in more sophisticated DDoS attack techniques, such as DNS water torture and carpet-bombing attacks, indicates an increased persistence of adversaries in finding and weaponizing new methods of attack. The documentation of nearly 500% growth in HTTP/S application layer attacks since 2019 and a significant rise in DNS reflection/amplification volumes during the first half of 2023 also points to an evolving threat landscape.

The narrative that emerges from these findings is one of a complex and adaptive threat environment where DDoS attacks are used as tools of geopolitical expression and are influenced by the advancement and deployment of technology infrastructure across the globe. This story of DDoS attack trends over the past five years reflects a world increasingly interconnected and at the same time vulnerable to the disruptions of cyber warfare.

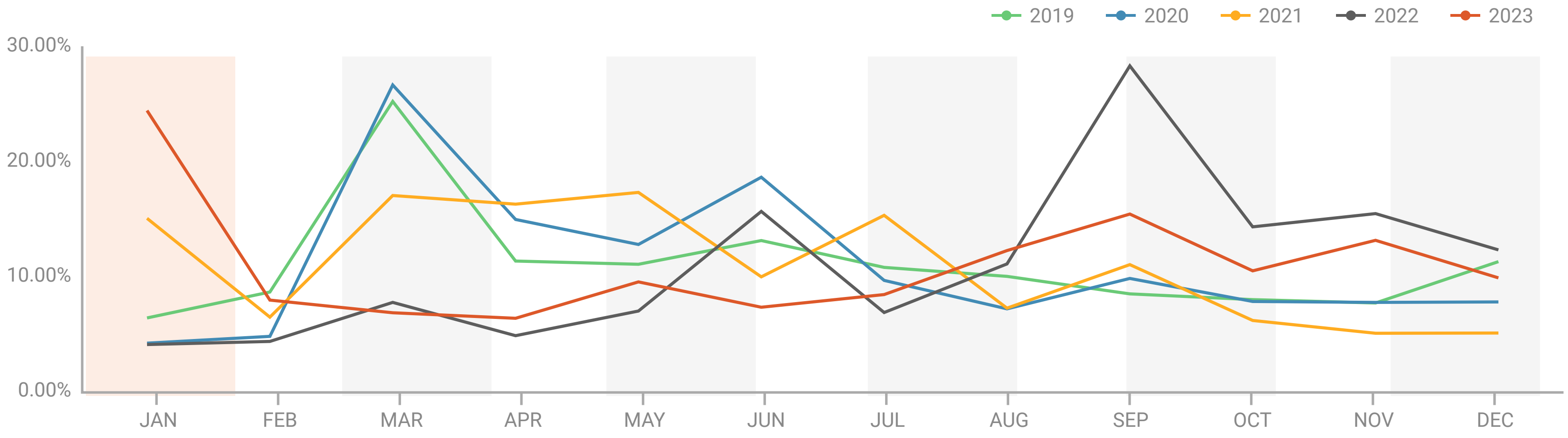


Figure 1 - DDoS Attack Trends from 2019 to 2023

2023 Attack Statistics

2023 Attack Statistics

Attack Vector Distribution

In 2023, the landscape of DDoS attacks was dominated by a trio of methods: NTP Amplification, HTTPS Flood, and DNS Amplification attacks, each playing a distinct role in shaping the cyber threat environment.

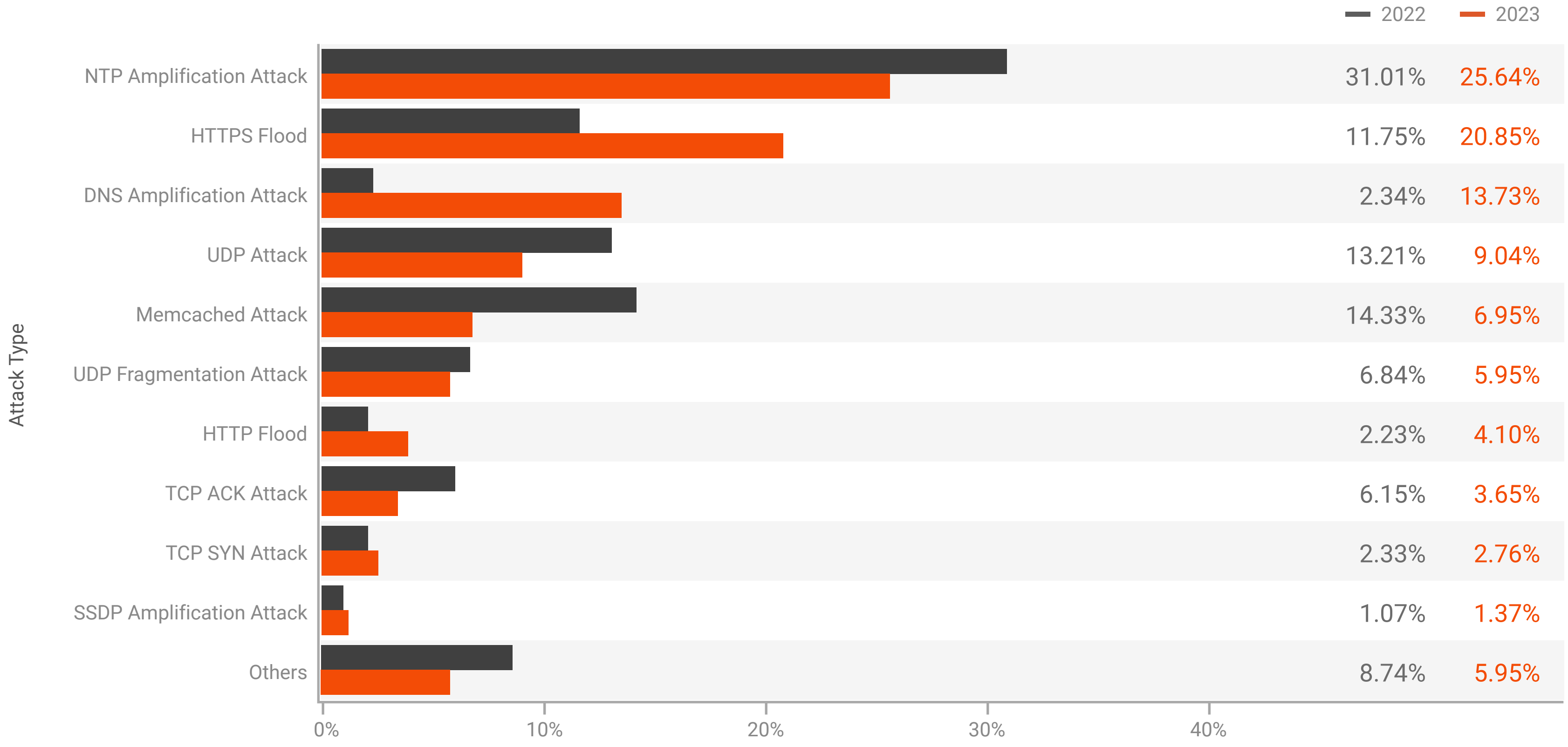


Figure 2 - Distribution of Attack Vector in 2022 and 202

2023 Attack Statistics

Top 3 Attack Vectors

NTP Amplification Attack

NTP Amplification attacks emerged as the leading protagonist in this domain. These attacks leveraged the Network Time Protocol's vulnerability to amplify the attack bandwidth significantly. This technique allowed attackers to launch massive attacks using limited resources, thereby causing substantial disruption with minimal effort. However, the story of NTP Amplification attacks in 2023 was also one of decline, with a 17.32% drop in occurrence. This change suggests a successful counter-narrative, where improved network configurations and heightened security awareness mitigated their impact.

HTTPS Flood

HTTPS Flood attacks, comprising 20.85% of the total, showcased a different tactic. These attacks targeted the secure web layer, overloading servers with a barrage of encrypted requests. This method's subtlety lies in its ability to mimic legitimate traffic, making detection and mitigation more challenging. Yet, even here, the plot thickened with a notable increase in these attacks by 77.47%.

DNS Amplification Attack

DNS Amplification attacks, accounting for 13.73% of the attacks, remained a significant concern. These attacks exploited open DNS servers to create large-scale disruptions. Despite ranking third, their persistence highlighted a continued vulnerability in global internet infrastructure, emphasizing the ongoing challenge for organizations to secure their networks against such widespread exploitation.

Amplification Attacks still top favorites

The narrative of the most popular attacks in 2023 was marked by evolving strategies, both in the form of attack methods and the corresponding defensive measures. Volumetric attacks in the form of highly efficient Amplification attacks remain the attacks of choice, but is best coupled with application layer HTTPS Flood attacks - pointing towards a dynamic cyber defense landscape, where adaptation and resilience play key roles.

2023 Attack Statistics

Attacks by Category Distribution

The landscape of DDoS attacks showcased significant trends and real-world incidents, particularly in the categories of Volumetric (Amplification) attacks, Application attacks, and Volumetric (Direct Flood) attacks.

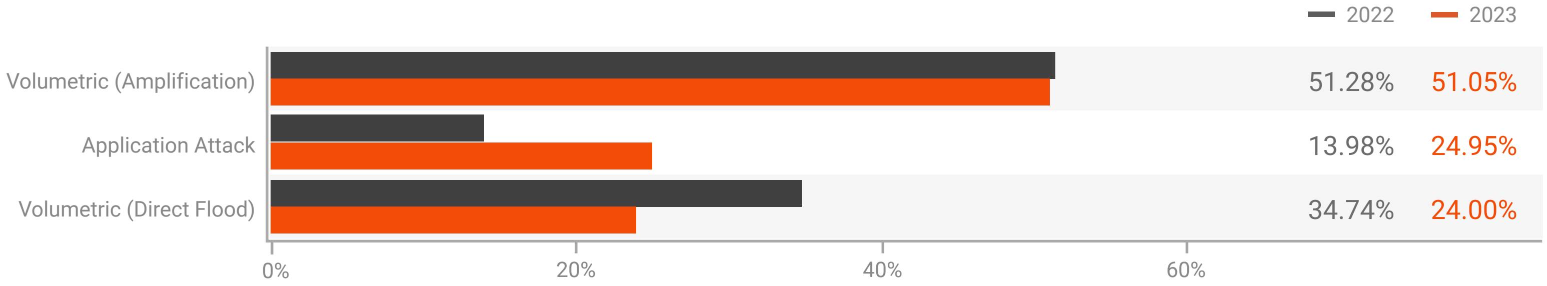


Figure 3 - Distribution of Attacks by Category in 2022 and 2023

Amplification attacks

-0.44%

Application attacks

+78.51%

Direct Flood attacks

-30.93%

Volumetric (Amplification) Attacks

While Volumetric (Amplification) attacks decreased by 0.44% YoY, they still represented a significant portion (51.05%) of DDoS incidents. A notable instance in 2022, which could be reflective of trends extending into 2023, was a massive volumetric attack mitigated by Nexusguard. This attack lasted for more than 36 hours with a sustained rate of over 700 Gbps. The combination of its duration, volume, packet rates and sustained attack rates made it one of the most significant DDoS attacks on our records. The growing number of internet-connected devices and available bandwidth also suggest that such large-scale volumetric attacks could continue to be a significant threat in the future.

Application Attacks

In 2023, the percentage of Application attacks among DDoS attacks was 24.95%, reflecting an increase of 78.51% YoY. These attacks are becoming more frequent and sophisticated, as seen with the rise of Application (HTTP/HTTPS) based attacks by groups like Killnet. These attacks have reached peaks of 294k requests per second and have shown the capability to adapt and re-tool approaches in response to emerging defenses.

Volumetric (Direct Flood) Attacks

Volumetric (Direct Flood) attacks accounted for 24.00% of the total attacks in 2023, witnessing a decrease of 30.93% YoY. This trend might be linked to improved network infrastructures capable of absorbing larger volumes of traffic or a shift in attacker strategies towards more sophisticated methods.

Technology, Finance, Banking & Insurance frequently targeted.

The prevalence of Application and Multi-vector attacks in these sectors suggests a focus on denying service to specific applications. These observations, combined with historical data, highlight a dynamic and evolving threat landscape in the realm of DDoS attacks and underscore the necessity for continuous adaptation and enhancement of cybersecurity defenses across various industries.

2023 Attack Statistics

Attacks by Protocol Distribution

In 2023, the DDoS attack landscape was significantly shaped by UDP and TCP-based attacks, while ICMP attacks were relatively less prominent. UDP-based attacks, known for sending numerous UDP packets to overwhelm targets, were the most dominant, accounting for 66.81% of the total attacks.

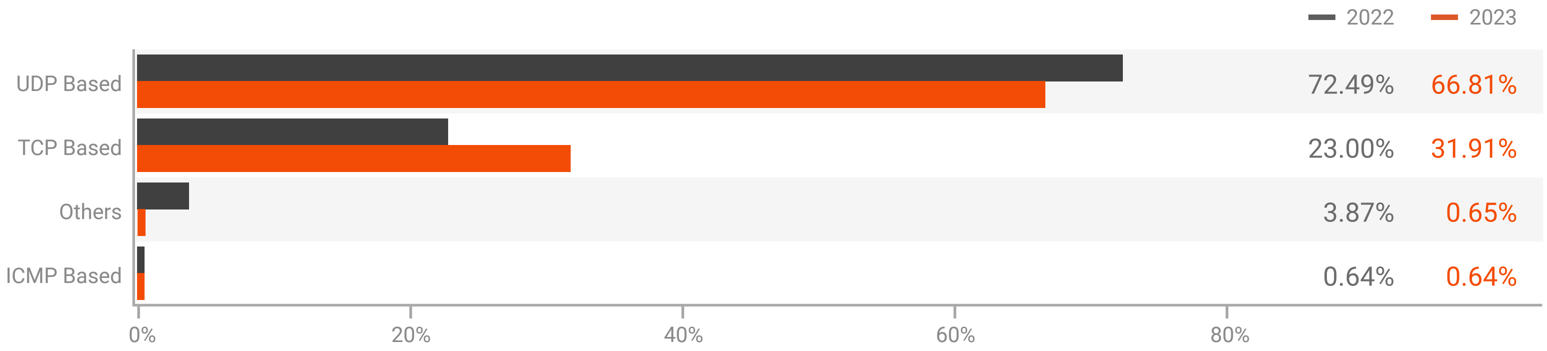


Figure 4 - Distribution of Attacks by Protocols in 2022 and 2023

UDP based attacks

-7.84 %

TCP based attacks

+38.75 %

ICMP based attacks

-0.95 %

TCP-based attacks

TCP-based attacks, comprising 33.91% of DDoS incidents, often involve initiating a high volume of TCP connection requests to deplete a target's resources. The financial sector in the UK, for example, experienced an upsurge in such attacks amid geopolitical tensions related to the Ukraine conflict. These attacks aimed to disrupt financial services, indicating a growing trend of targeting critical economic infrastructures. The year-on-year increase of 38.75% in TCP-based attacks implies an enhancement in detection and mitigation strategies.

ICMP-based attacks

ICMP-based attacks, although constituting a smaller fraction (0.64%) of the total, were part of the overall DDoS threat spectrum. These attacks typically involve flooding the target with ICMP echo requests, leading to resource exhaustion.

A Game of Cat & Mouse

The decline in the predominant attack types of the year reflects a dynamic attack-defense landscape, where organizations are increasingly capable of responding to and mitigating such threats, which in turn propels the continuous evolution in the methods and strategies employed by cyber attackers to stay ahead of the game.

2023 Attack Statistics

Quantity of Attack Vectors

The prevalence of single-vector attacks at 92.70% of total DDoS attacks, compared to multi-vector attacks in 2023, suggests a significant trend in the cyber threat landscape. There are several potential reasons for this predominance of single-vector attacks:

Simplicity and Cost-Effectiveness: Single-vector attacks are generally simpler to execute and require fewer resources. The simplicity also means that less technical expertise is required, making these attacks more accessible to a broader range of attackers.

Sufficient Effectiveness: For many targets, a single-vector attack can be sufficiently effective to disrupt operations or services. If the primary goal of the attack is to cause disruption or downtime, even a straightforward attack method like a UDP flood can be effective without the need for more sophisticated multi-vector approaches.

Detection Evasion: While it might seem counterintuitive, single-vector attacks can sometimes be more difficult to detect and mitigate due to their straightforward nature. They can more easily blend in with legitimate traffic, making it harder for defense systems to identify and block the attack without affecting normal operations.

Shift in Attacker Priorities: The prevalence of single-vector attacks could also reflect a shift in attacker priorities or strategies. As cybersecurity defenses evolve, attackers might be adapting their methods, possibly finding that single-vector attacks meet their objectives with lower risk or effort.

Resource Allocation: Conducting multi-vector attacks requires more resources, coordination, and technical know-how. Attackers might reserve such complex attacks for high-value targets or specific campaigns, whereas single-vector attacks are more broadly utilized for a range of targets.

Evolution of Defense Mechanisms: The evolution of defense mechanisms against multi-vector attacks might also be a contributing factor. As multi-vector attacks have historically posed significant threats, organizations might have developed more robust defenses against them, leading attackers to pivot back to single-vector attacks.

It's important to note that while single-vector attacks dominate, the presence of multi-vector attacks, though in the minority, indicates a continued need for comprehensive and adaptive defense strategies. Multi-vector attacks, due to their complexity, can be particularly challenging to defend against and may be employed in more targeted and sophisticated cyber campaigns.

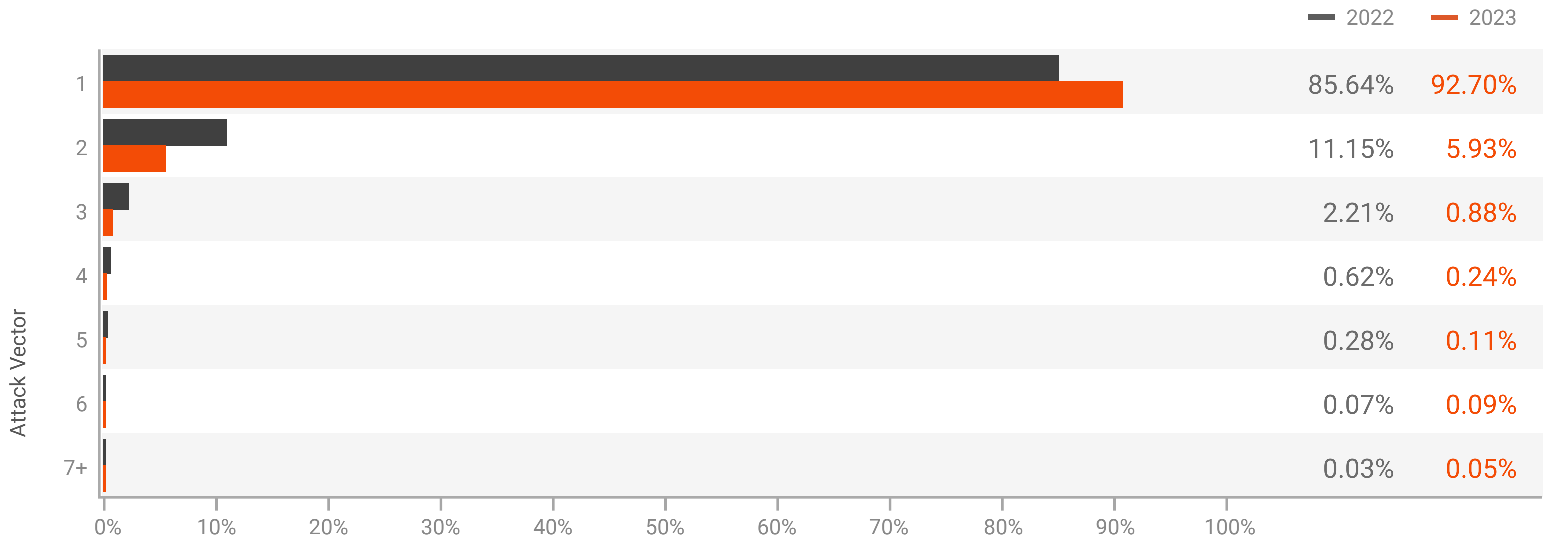


Figure 5 - Distribution of DDoS Attack Vectors in 2022 and 2023

Single-vector attacks

93%

Multi-vector attacks

7%

2023 Attack Statistics

Multi-Vector Attack Combinations

The data in this section illustrates the distribution of common multi-vector DDoS attack combinations. Multi-vector DDoS attacks leverage multiple attack vectors simultaneously, making them more complex and harder to defend against compared to single-vector attacks.

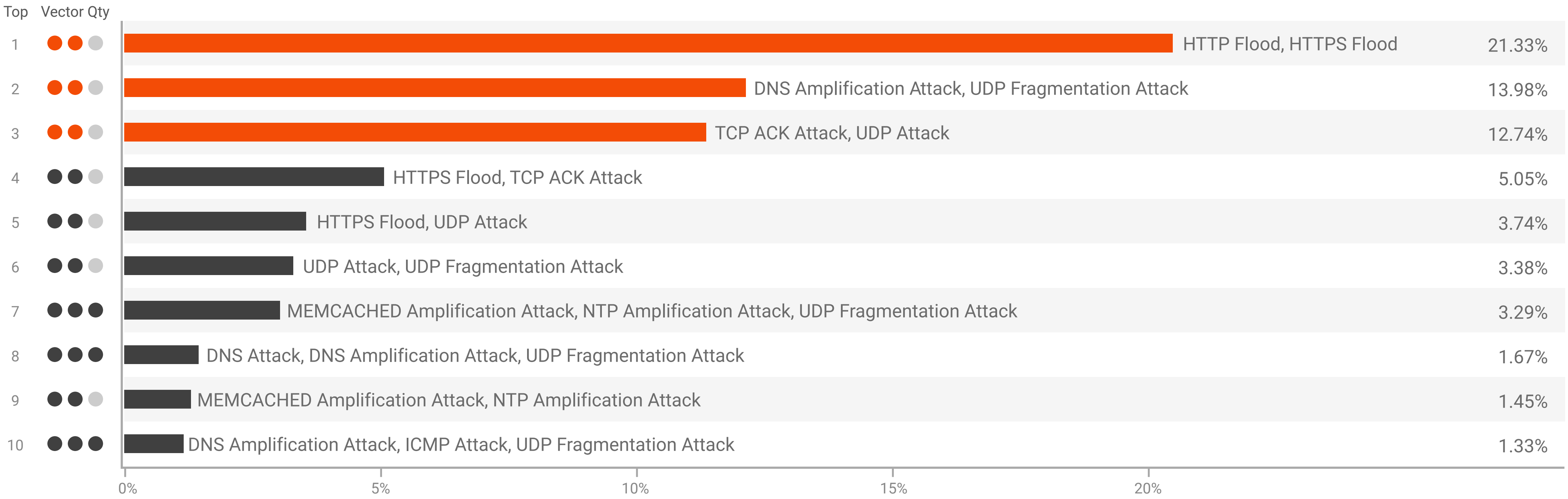


Figure 6 - Top 10 multi-vector combinations in 2023

2023 Attack Statistics

Top 3 Multi-Vector Attack Vectors

HTTP and HTTPS Floods

These attacks target web servers and applications by overwhelming them with HTTP or HTTPS requests.
The fact that this combination is the most common (21.33%) underscores the vulnerability of web services to DDoS attacks.

DNS Amplification and UDP Fragmentation

This combination leverages the amplification factor of DNS queries to generate massive volumes of UDP traffic, overwhelming the target's network infrastructure. A past instance of such an attack was observed in the Dyn cyberattack in 2016, which took down major websites like Twitter, Netflix, and PayPal. This attack didn't solely rely on DNS amplification but demonstrated how potent such techniques could be when combined.

TCP ACK Attack and UDP Attack

Combining TCP ACK and UDP attack vectors can disrupt both stateful and stateless firewall processing capabilities.
Real-world examples of such attacks are less commonly reported in the media but are frequent in online gaming and service provider networks, aiming to disrupt services or extort victims.

Beyond Modern Mitigation

The Mirai botnet, known for its massive scale IoT device exploitation, has been used for various complex multi-vector attacks, showcasing the evolution of attack methodologies.

As attackers continue to refine their tactics, organizations must enhance their resilience against such threats through improved detection, mitigation technologies, and by understanding the nature and mechanisms of these attacks.

2023 Attack Statistics

Attack Duration Distribution

In a comprehensive analysis of Distributed Denial of Service (DDoS) attack durations for the years 2022 and 2023, notable trends emerge that reflect the evolving cybersecurity landscape. DDoS attacks, designed to overwhelm websites and online services, rendering them inaccessible, have long been a tool for cybercriminals. However, the data from these two years provides insight into how the nature of these attacks is changing, likely influenced by advancements in defense mechanisms, shifts in attacker tactics, regulatory impacts, and increased organizational preparedness.

Key Findings:

- Attacks lasting 90 minutes increased by 22.20%.
- There was an increase in the proportion of attacks falling within the 90-240 minute range, which accounted for 2.11%.
- Attacks in the 240-420 minute range increased from 67.96%, indicating a possible shift in attacker preferences or tactics within this range.
- The occurrence of attacks lasting between 420-720 minutes and 720-1200 minutes decreased by 2.19% and increased 32.53% respectively.
- Lastly, the duration of the longest attacks (1200+ minutes) saw a reduction from 95.03% of the total event count.

Duration (Minutes)

	2022	2023
Maximum	27642.12	24267.33
Average	82.76	101.10

Table 1 - Maximum and Average duration between 2022 and 2023

These trends suggest several underlying factors at play in the cybersecurity arena:

Enhanced Security Measures: Organizations worldwide have ramped up their cybersecurity defenses, incorporating sophisticated detection systems, strengthening infrastructure resilience, and deploying swift response strategies to mitigate DDoS attacks effectively.

Evolving Attacker Strategies: Cybercriminals may be adjusting their approaches, possibly pivoting from prolonged assaults to shorter, more intense bursts of activity or other forms of cyber threats that are more challenging to defend against and potentially more damaging.

Regulatory and Enforcement Actions: Increased regulatory scrutiny and proactive law enforcement efforts against cybercrime networks have likely disrupted the operations of many would-be attackers, curtailing their ability to launch extended DDoS campaigns.

Greater Awareness and Preparedness: The cybersecurity community's heightened awareness and preparedness for DDoS threats have likely led to improved mitigation capabilities. This proactive stance enables organizations to quell attacks more swiftly, thus reducing their overall duration.

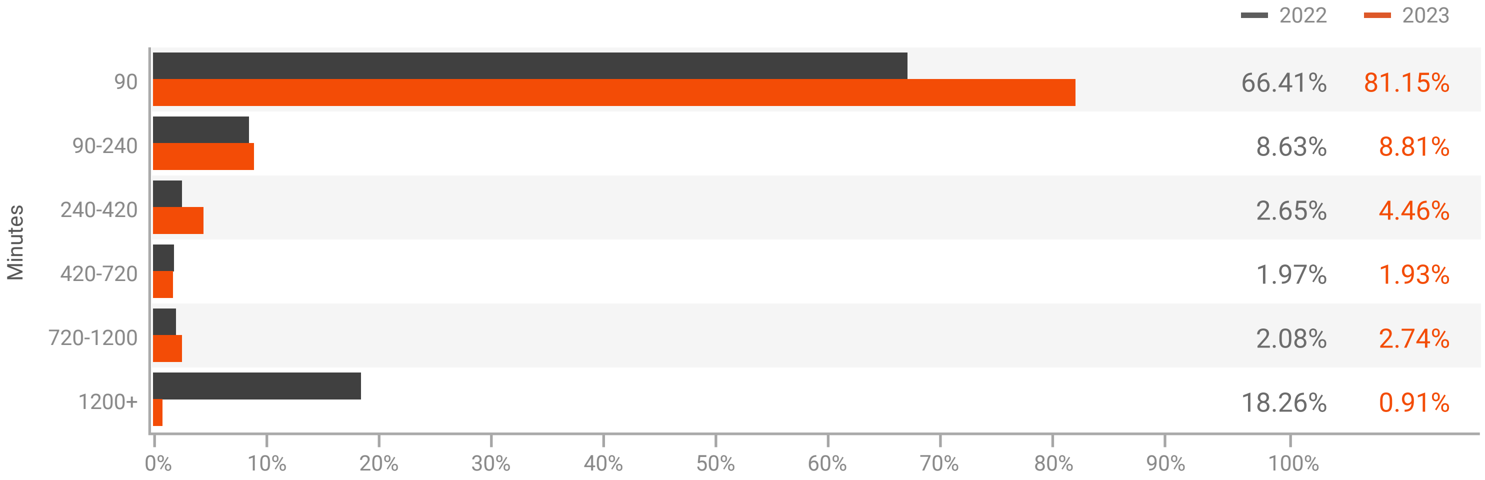


Figure 7 - Attack Durations Distribution in 2022 and 2023

81%

of attacks were shorter than 90 minutes

Gaining grounds in the Eternal Cyber Conflict

As major service providers and hosting companies invest heavily in DDoS mitigation technologies, often partnering with leading cybersecurity firms to bolster their defense, attacks are finding it increasingly difficult to sustain prolonged disruptions. Collaborative efforts by international law enforcement have also led to significant takedowns of botnets and individuals behind them.

The reduction in DDoS attack durations from 2022 to 2023 signals a positive trend in the ongoing battle against cyber threats. It underscores the importance of continued investment in cybersecurity defenses, the need for international cooperation in combating cybercrime, and the effectiveness of regulatory measures in protecting online spaces.

2023 Attack Statistics

Attack Size Distribution

In 2023, the landscape of Distributed Denial of Service (DDoS) attacks underwent notable changes compared to 2022. This section delves into the size of DDoS attacks observed during these years, highlighting trends, drawing comparisons, and exploring the underlying reasons for these shifts.

Data analysis reveals a significant shift in the distribution of DDoS attack sizes from 2022 to 2023. While the overall number of attacks decreased, there was a marked increase in the proportion of larger-scale attacks (>=10 Gbps). Specifically, attacks under 1 Gbps still constituted the majority but saw a decrease in their total count, indicating a possible shift towards more potent attacks.

Key Findings:

Decrease in Total Attacks: The total number of DDoS attacks saw a reduction in 2023. This 24.6% decrease suggests an evolving threat landscape where attackers might be opting for quality over quantity.

Shift Towards Larger Attacks: The most significant change was observed in the >=10 Gbps category, which saw an increase for 2023. This dramatic rise (over 450%) in larger-scale attacks signifies a concerning trend towards more disruptive and powerful attacks.

Proportional Changes: While smaller attacks (<1 Gbps) still dominate, their proportion slightly increased from 88.1% to 90.9%. Conversely, mid-sized attacks (>=1 and <10 Gbps) saw a decrease in both count and proportion, highlighting a polarization towards either end of the scale.

Several factors could contribute to the observed shift in DDoS attack sizes:

Advancements in Attack Technology: Attackers are leveraging more sophisticated tools and techniques, enabling them to launch larger and more effective attacks with less effort.

Increased Attack Surface: The expansion of IoT devices and cloud services provides attackers with more targets and opportunities to amplify their attacks.

Motivation and Impact: Larger attacks often generate more media coverage and can fulfill various motives, including extortion, political activism, or demonstrating capability.

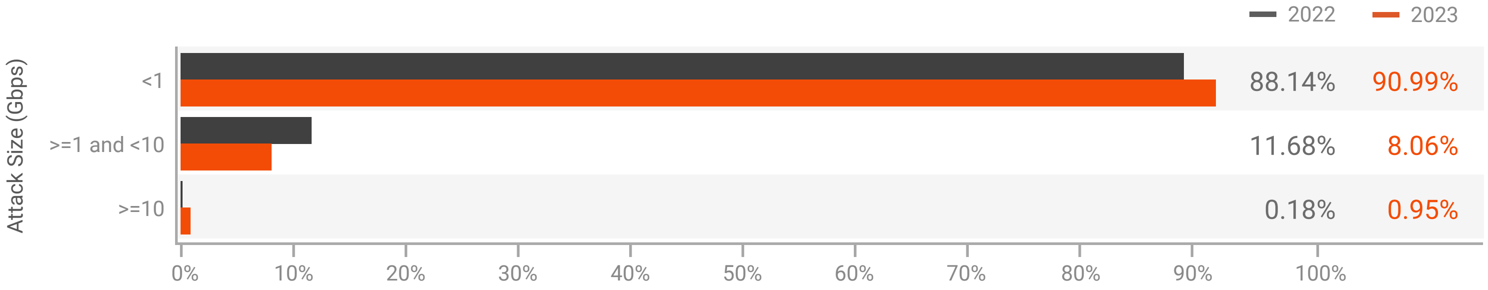


Figure 8 - Attack Size Distribution in 2022 and 2023

91%

of attacks were smaller than 1Gbps

The year 2023 marked a turning point in the nature of DDoS attacks, with a clear move towards larger, more destructive efforts. This evolution demands heightened awareness and enhanced security measures from organizations worldwide. As attackers continue to refine their strategies, the need for robust defense mechanisms and international cooperation becomes ever more critical.

2023 Attack Statistics

The State of Bit- and- Piece DDoS Attacks in 2023

In 2023, Distributed Denial of Service (DDoS) attacks notably evolved in complexity and impact, with Bit-and-Piece (BNP) attacks emerging prominently. These attacks employ small data packets from diverse sources to flood systems, challenging to detect and mitigate. Data shows 214 Autonomous System Numbers (ASNs) were hit by 1,177 BNP DDoS incidents, leveraging amplification methods like CHARGEN, SSDP, DNS, and NTP, impacting various countries including Australia, Bangladesh, Brazil, and Bulgaria.

Summary 1 - Bit-and-Piece Attacks in 2022 and 2023

		2022	2023	Difference
No. of Targeted ASN		240	214	-10.83%
No. Target Geolocations		20	30	50.00%
Total IP prefixes under attack(Class C)		3,079	1,177	-61.77%
No. of targeted IP addresses per IP prefix	Minimum	30	30	0.00%
	Maximum	256	256	0.00%
Attack Duration(Minutes)	Minimum	2.00	13.18	599.0%
	Maximum	2,577.00	1,571.65	-39.01%
Attack Count per IP	Minimum	40	40	0.00%
	Maximum	74,570	8,124	-89.11%
Attack Count per IP Prefix	Minimum	441	1,278	189.80%
	Maximum	3,366,723	63,245,641	1778.55%
Attack Size by IP (Gbps)	Minimum	0.0004	0.0020	400.00%
	Maximum	21.38	49.82	133.02%
Attack Size by IP Prefix /24 (Gbps)	Minimum	0.0297	0.0245	-17.51%
	Maximum	123.72	178.06	43.92%

Targeted ASNs

214

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

1,177

Summary 2 - Bit-and-Piece Attack Types

2022

- SSDP Amplification Attack(44.75%)
- NTP Amplification Attack(20.14%)
- Memcached Attack(10.89%)
- CHARGEN Attack(6.86%)
- UDP Fragmentation Attack(6.15%)
- DNS Amplification Attack(2.50%)
- UDP Attack(1.62%)
- TCP ACK Attack(1.59%)
- ICMP Attack(0.88%)
- TCP SYN Attack(0.69%)
- SNMP Amplification Attack(0.52%)
- IP BOGONS(0.47%)
- TCP RST Attack(0.44%)
- TCP Null Attack(0.38%)
- TCP Fragmentation Attack(0.38%)
- HTTP Flood(0.36%)
- WS-DISCOVERY Amplification Attack(0.36%)
- CLDAP Reflection Attack(0.27%)
- HTTPS Flood(0.19%)
- BITTORRENT Amplification Attack(0.19%)
- L2TP Amplification Attack(0.16%)
- IP Fragmentation Attack(0.11%)
- DNS Attack(0.05%)
- SIP Flood(0.03%)
- STEAM PROTOCOL Amplification Attack(0.03%)

2023

- CHARGEN Amplification Attack(46.67%)
- SSDP Amplification Attack(18.39%)
- NTP Amplification Attack(11.58%)
- UDP Fragmentation Attack(8.28%)
- MEMCACHED Amplification Attack(6.52%)
- DNS Amplification Attack(4.25%)
- UDP Attack(1.47%)
- TCP SYN Attack(1.25%)
- WS-DISCOVERY Amplification Attack(0.81%)
- TCP SYN-ACK Attack(0.37%)
- TCP ACK Attack(0.15%)
- L2TP Amplification Attack(0.15%)
- ICMP Attack(0.07%)
- DNS Attack(0.07%)

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

2022	2023
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	Australia, Bangladesh, Brazil, Bulgaria, Cambodia, China, Czechia, France, Germany, Hong Kong, Indonesia, Iran, Japan, Libya, Lithuania, Netherlands, Pakistan, Paraguay, Romania, Russian Federation, Slovenia, Spain, Sweden, Taiwan, Tunisia, Turkey, United Arab Emirates, United Kingdom, United States, Vietnam

The Challenge for CSPs

CSPs play a critical role in the digital ecosystem, providing essential infrastructure for internet connectivity and services. The increasing frequency and sophistication of Bit- and-Piece DDoS attacks put immense pressure on CSPs to evolve their defense mechanisms. This includes deploying more advanced detection technologies, enhancing network resilience, and adopting a more proactive and collaborative approach to cybersecurity.

Recommendations

Enhanced Detection and Mitigation:
CSPs need to invest in advanced detection technologies that can identify and mitigate Bit-and-Piece attacks in real-time. Machine learning and AI-driven solutions can offer the ability to adapt to evolving attack patterns.

Collaboration:
Collaboration among CSPs, as well as with governments and international cybersecurity organizations, is crucial for sharing threat intelligence and best practices for defense.

Customer Education:
Educating customers on the risks of DDoS attacks and promoting the use of security services can help reduce the impact of attacks.

Regulatory Compliance and Best Practices:
Adhering to industry standards and regulatory requirements can guide CSPs in implementing robust cybersecurity frameworks.

A Call for Unified CSP Defense

The data highlights the significant challenge Bit-and-Piece DDoS attacks pose to CSPs globally. As these attacks continue to evolve in complexity and scale, CSPs must adopt a multifaceted and collaborative approach to cybersecurity. This includes leveraging advanced technologies, enhancing operational resilience, and fostering industry-wide cooperation to effectively mitigate the threat of DDoS attacks and ensure the reliability and security of communication services.

2023 Attack Statistics

Source Distribution of Application Attacks[1]

The findings in this section indicate a significant shift in the source distribution of Application Layer DDoS attacks from 2022 to 2023. A striking increase in attacks originating from devices running Windows OS is evident, suggesting a pivot in attacker strategies or an increase in the vulnerability of these systems.

Key Findings:

Increase in Attacks from Windows OS Devices: There was a dramatic rise in the number of attacks from devices running Windows OS, indicating that these devices might have been more targeted or that there was an increase in malware affecting Windows systems.

Change in Device Types: The data may also reveal changes in the types of devices used for attacks, such as an increase in attacks from computers and servers compared to mobile devices or IoT devices, reflecting shifts in attacker preferences or the discovery of new vulnerabilities.

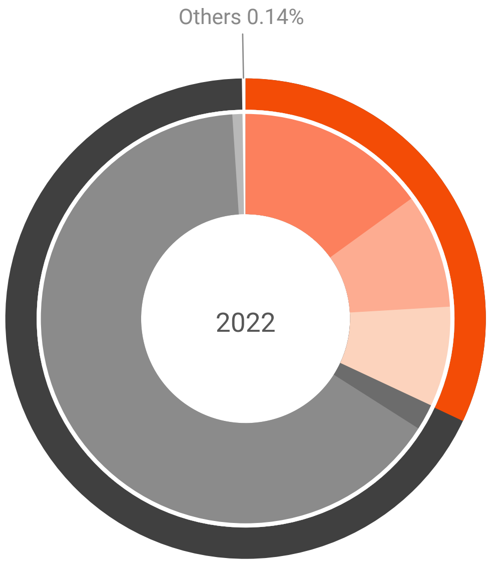
Contributing Factors Behind the Trends

Vulnerability Exploitation: New vulnerabilities discovered in Windows OS or more sophisticated malware might have made it easier to compromise these systems.

Botnet Evolution: The evolution of botnets, with attackers favoring more powerful computing resources provided by computers and servers, particularly those running Windows OS, for more effective attacks.

Shift in Attacker Tactics: Attackers might have shifted tactics due to changes in cybersecurity defenses, targeting devices and operating systems perceived as less secure or more widely used in corporate environments.

[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.



Source Distribution of Application Attacks

	2022	2023
🟧 **Computers and Servers**	**31.98%**	**92.25%**
🟧 Windows OS	15.42%	87.82%
🟧 Macintosh OS	8.71%	2.58%
🟧 Other OS	7.85%	1.85%
⬛ **Mobile Devices**	**67.88%**	**7.72%**
⬛ iOS	2.25%	2.79%
⬛ Android	65.53%	4.90%
⬛ BlackBerry, DoCoMo	0.10%	0.03%
□ **Others** Other OS e.g. PSP, Nintendo Wii, Nintendo DS	**0.14%**	**0.03%**

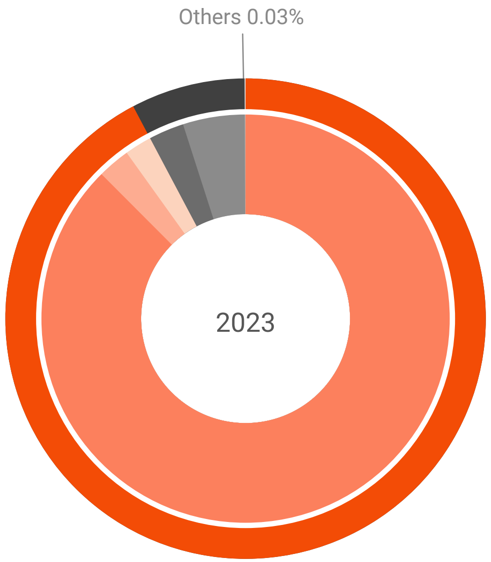


Figure 9 - Source Distribution of Application Attacks in 2022 and 2023

No system is Infallible

The shift in primary attack sources to Windows OS devices, reflects the dynamic nature of cyber threats. It emphasizes the need for ongoing vigilance, software updates, and reinforced cybersecurity defenses for all systems and networks. Real-world examples in 2023, such as the exploitation of Microsoft Exchange Server vulnerabilities and the rise of ransom DDoS attacks, serve as stark reminders of the tangible impacts of these attacks. As attackers evolve, we must adapt our defense and resilience strategies against DDoS attacks.

2023 Attack Statistics

Application Attack Source Distribution (IP Reputation)

Top 10 Attack Sources Ranking in APAC (2023)

	2023
China	91.49%
Singapore	3.12%
Thailand	0.97%
India	0.87%
Indonesia	0.76%
Hong Kong	0.66%
Taiwan	0.39%
Japan	0.25%
Australia	0.22%
Malaysia	0.22%
Others	1.05%

Top 10 Attack Sources Ranking in Europe (2023)

	2023
Russian Federation	21.93%
United Kingdom	15.37%
Germany	14.53%
Netherlands	8.96%
France	8.06%
Spain	3.20%
Poland	3.20%
Ukraine	2.95%
Italy	2.69%
Ireland	2.12%
Others	16.99%

Top 10 Attack Sources Ranking in Middle East and Africa (2023)

	2023
Turkey	66.89%
Tanzania, United Republic of	5.46%
Iran	5.11%
Mozambique	3.32%
Israel	3.27%
Kenya	2.65%
South Africa	1.95%
Nigeria	1.17%
Morocco	0.96%
Egypt	0.96%
Others	8.26%

Top 10 Attack Sources Ranking in America (2023)

	2023
United States	60.43%
Brazil	29.83%
Canada	3.66%
Mexico	1.12%
Argentina	1.08%
Colombia	0.74%
Ecuador	0.40%
Belize	0.38%
Peru	0.34%
Venezuela	0.32%
Others	1.70%

Geo-Political Undercurrents Drive DDoS Attacks

The prominence of these countries in DDoS attack distribution is not solely a matter of technological infrastructure but also reflects socio-economic factors, cybersecurity practices, and geopolitical considerations. For instance, lax cybersecurity regulations, inadequate defense mechanisms, and the presence of large numbers of unsecured devices contribute to the volume of attacks originating from these regions. This 2023 data on DDoS attack sources underscores the complex, multifaceted nature of cyber threats. Understanding the reasons behind the geographic distribution of these attacks is crucial for developing effective countermeasures.

2023 Attack Statistics

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

Top 10 ASN Attacks Ranking (2023)

	AS Name	2023
14061	DIGITALOCEAN-ASN, US	3.78%
16509	AMAZON-02, US	3.73%
9808	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd., CN	3.66%
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	3.11%
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	2.71%
4766	KIXS-AS-KR Korea Telecom, KR	1.79%
213230	HETZNER-CLOUD2-AS, DE	1.45%
40065	CNSERVERS, US	1.27%
17547	M1NET-SG-AP M1 NET LTD, SG	1.26%
24940	HETZNER-AS, DE	1.07%
Others		76.16%

Top 10 ASN Attacks Ranking in APAC (2023)

	AS Name	2023
9808	CHINAMOBILE-CN China Mobile Communications Group Co., Ltd., CN	8.45%
4837	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN	7.17%
4134	CHINANET-BACKBONE No.31,Jin-rong Street, CN	6.24%
4766	KIXS-AS-KR Korea Telecom, KR	4.13%
17547	M1NET-SG-AP M1 NET LTD, SG	2.89%
132203	TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN	2.43%
7713	TELKOMNET-AS-AP PT Telekomunikasi Indonesia, ID	2.22%
45090	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	2.20%
63949	AKAMAI-LINODE-AP Akamai Connected Cloud, SG	1.78%
9231	IPEOPLESNET-AS-AP China Mobile Hong Kong Company Limited, HK	1.70%
Others		60.79%

Top 10 ASN Attacks Ranking in Europe (2023)

	AS Name	2023
213230	HETZNER-CLOUD2-AS, DE	7.95%
24940	HETZNER-AS, DE	5.86%
60729	ZWIEBELFREUN, DE	3.05%
51167	CONTABO, DE	2.83%
212317	HETZNER-CLOUD3-AS, DE	2.45%
16276	OVH, FR	2.37%
9009	M247, RO	2.28%
31083	TELEPOINT, BG	2.17%
12389	ROSTELECOM-AS, RU	2.06%
35830	BTTGROUP-AS, GB	1.79%
Others		67.20%

Top 10 ASN Attacks Ranking in Middle East and Africa (2023)

	AS Name	2023
34984	TELLCOM-AS, TR	7.27%
21003	GPTC-AS, LY	4.70%
202561	HIGHSPEED, TR	4.52%
44217	IQNETWORKS, IQ	3.79%
9121	TTNET, TR	3.65%
47331	TTNET, TR	3.64%
37284	Aljeel-net, LY	3.10%
42337	RESPINA-AS, IR	2.69%
22750	BCSNET, ZA	2.21%
12735	ASTURKNET, TR	2.20%
Others		62.21%

Top 10 ASN Attacks Ranking in America (2023)

	AS Name	2023
14061	DIGITALOCEAN-ASN, US	11.46%
16509	AMAZON-02, US	11.33%
40065	CNSERVERS, US	3.86%
35913	DEDIPATH-LLC, US	3.23%
15169	GOOGLE, US	1.99%
6500	NEXUS-22-6500, US	1.95%
8151	UNINET, MX	1.87%
36351	SOFTLAYER, US	1.72%
20473	AS-CHOOPA, US	1.61%
11878	TZULO, US	1.51%
Others		59.48%

Reflected Attack Destination Distribution

This section outlines the distribution of targets of Reflected DDoS attacks by country for the year 2023. This analysis aims to shed light on the global landscape of cyber threats, particularly focusing on the countries that are most targeted by these types of attacks. By correlating these findings with real-world cases and trends observed, we provide insights into the possible reasons behind the distribution of these attacks and their significance.

Top Targeted Countries

The analysis reveals that Pakistan, Brazil, Libya, and the United States are the top countries targeted by Reflected DDoS attacks in 2023. Specifically, Pakistan leads with a significant margin, followed by Brazil, Libya, and the United States. This distribution suggests a diverse geopolitical and economic landscape of targeted countries, ranging from South Asia and Latin America to the Middle East and North America.

Significance of these Findings

Pakistan as the leading target of Reflected DDoS attacks is particularly noteworthy. The country's burgeoning digital infrastructure, coupled with its strategic geopolitical position, might make it a focal point for cyber-attacks. These attacks could be motivated by a range of factors, including political, military, or cyber espionage intentions, reflecting the broader regional tensions and global cyber warfare trends.

Brazil's position as the second most targeted country highlights the growing trend of cyber-attacks in South America. Brazil's significant internet population and its role as a leading economy in the region may make it an attractive target for cybercriminals looking to disrupt commercial and government services or for hacktivist groups aiming to make political statements.

Libya, ranking third, underscores the impact of political instability on cyber security. The ongoing political and military conflicts within the country likely contribute to its vulnerability to cyber-attacks. Such a scenario provides a fertile ground for cybercriminals to exploit weakened cybersecurity defenses.

The United States being among the top targeted countries aligns with its status as a global superpower with extensive digital and physical infrastructure. The motivations for targeting the US are manifold, including state-sponsored cyber espionage, cybercrime, and ideological motivations by non-state actors.

Correlation with Real-World Cases

The prominence of these countries in the context of Reflected DDoS attacks correlates with several real-world cybersecurity incidents reported over the past year. For example, there have been instances where political tensions have escalated into the cyber domain, with state-sponsored and independent hacker groups launching attacks against nations as a form of digital warfare or protest. The financial and data-rich targets in these countries also make them attractive for cybercriminal activities aiming for financial gain or disruption of critical services.

Why These Findings Matter

Understanding the distribution of Reflected DDoS attacks is crucial for several reasons:

- It helps in identifying vulnerable regions and sectors that may require enhanced cybersecurity measures.
- It provides insights into potential geopolitical and economic motivations behind cyber-attacks, aiding in the development of more effective national and international cybersecurity policies and strategies.
- It emphasizes the need for international cooperation in combating cyber threats, which often transcend national borders.

Top 10 Reflected Attack Destinations in APAC (2023)

	Percentage
Bangladesh	69.38%
China	20.67%
Hong Kong	5.50%
Singapore	3.46%
Australia	0.52%
India	0.18%
Japan	0.10%
South Korea	0.06%
Malaysia	0.05%
Philippines	0.02%
Others	0.06%

Top 10 Reflected Attack Destinations in Europe (2023)

	Percentage
Germany	36.51%
United Kingdom	13.55%
France	9.43%
Russian Federation	7.37%
Czechia	5.73%
Poland	5.16%
Romania	3.79%
Netherlands	3.21%
Belgium	2.97%
Lithuania	1.77%
Others	10.51%

Top 10 Reflected Attack Destinations in Middle East and Africa (2023)

	Percentage
Libya	95.06%
Seychelles	2.91%
Mauritius	1.15%
Saudi Arabia	0.55%
Réunion	0.12%
Iran	0.04%
United Arab Emirates	0.04%
South Africa	0.03%
Bahrain	0.03%
Algeria	0.02%
Others	0.05%

Top 10 Reflected Attack Destinations in America (2023)

	Percentage
Brazil	45.90%
United States	41.92%
Argentina	8.82%
Canada	1.73%
Chile	1.09%
Belize	0.19%
Colombia	0.18%
Ecuador	0.13%
Dominican Republic	0.03%
British Virgin Islands	0.01%
Others	0.00%

Conclusion

The 2024 Annual DDoS Trend Report has unveiled a nuanced landscape of Distributed Denial of Service (DDoS) attacks, characterized by evolving attack vectors, shifting geopolitical motives, and the increasing sophistication of cyber threats. Despite a marked decrease in the total number of DDoS attacks, our analysis highlights a strategic pivot towards larger, more impactful attacks, suggesting an alarming trend towards maximizing damage and disruption.

Our findings underscore the universal risk DDoS poses across industries, with notable increases in attack sizes and the emergence of sophisticated multi-vector attack combinations. The politicization of DDoS tactics, especially through hacktivism, further complicates the threat landscape, intertwining cybersecurity with national security and international relations.

This report serves as a strategic blueprint for organizations aiming to navigate the complexities of DDoS threats. The decline in certain types of attacks, alongside the rise in others, calls for a dynamic and adaptive approach to cybersecurity defenses.

Looking Ahead: Strategies for Mitigation and Preparedness

Enhanced Threat Intelligence: Organizations must invest in real-time threat intelligence to stay ahead of evolving DDoS tactics and strategies. Understanding attacker motivations and tactics is crucial for developing effective defense mechanisms.

Robust Infrastructure Resilience: Building resilience into digital infrastructure can mitigate the impact of attacks. This includes diversifying network resources, adopting cloud-based DDoS mitigation strategies, and ensuring redundancy in critical systems.

Collaborative Defense Mechanisms: Collaboration among businesses, governments, and international entities is essential for sharing intelligence, best practices, and resources. Collective efforts can lead to the development of more effective strategies to combat DDoS threats globally.

Public Awareness and Education: Raising awareness about the importance of cybersecurity hygiene and the risks associated with DDoS attacks can empower individuals and organizations to take proactive measures in protecting their digital assets.

Policy and Regulatory Frameworks: Governments and regulatory bodies must establish comprehensive cybersecurity frameworks that encourage the adoption of best practices, promote reporting and information sharing, and facilitate coordinated responses to cyber threats.

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 Trend Report.

20240321-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