zayo

Protecting Your Business From Cyber Attacks

The State of DDoS Attacks

DDoS Insights:

2023 – End of Year Review

Executive Summary

Large fluctuations in DDoS attack activity quarter over quarter through 2023 still point to a **16% overall increase** over the course of the year. Telecom, retail, healthcare, and government were hit especially hard.

In the second half of 2023, once again **telecommunications** companies experienced the **most frequent attacks**, comprising about 40% of total attack volume with nearly 13,000 attacks over the course of these 6 months.

An astonishing second quarter of attacks (up 387% from Q1), seems to have leveled in the second half of the year. Across all industries comparing Q4 to Q1 2023, companies saw a 16% increase in attack activity.

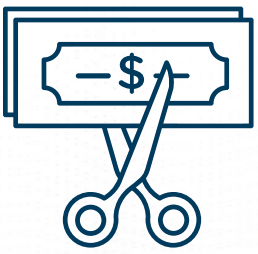
In the second half of 2023, **government** once again experienced the **longest attacks** with the average attack duration increasing from 4 hours in the first half of the year, to **18 hours** in the second half, representing an increase of 322%.

Across all industries, attackers are launching more persistent, longer attacks. The average duration of attacks increased by over 400% from Q1 to Q4 2023, from an average of 24 minutes per attack in Q1, to 121 minutes per attack in Q4.

Retail and **healthcare** companies experienced the **largest attacks** in the second half of the year, with an average attack size of **2.5 Gbps** across companies in these two industries.

Across all industries in the second half, attack size has dropped. However, even the smallest attack can cause business reputational – and financial – harm. Plus the drop in attack size points to a troubling emerging trend: the increasing use of multi-vector attacks.

Across all industries, organizations experienced 110 attacks on average over the 6 month time frame - **4 attacks every week.**



The Cost of Exposure: No matter the attack frequency, duration, or size, unprotected organizations experienced an average cost of $6,000 per minute of each DDoS attack.

Factors such as lost revenue, the cost of detection and recovery, legal fees, reputational harm, customer churn, opportunity costs during downtime, and many other factors, can easily surpass **$150,000 for a single 20-minute attack**.

DDoS 101

A Distributed Denial of Service (DDoS) attack is a deliberate cyber attack against an organization's online presence.

A DDoS attack, launched simultaneously from multiple systems, floods a victim's Internet circuit with fake or illegitimate traffic to prevent true user traffic from passing. DDoS attacks are more common than phishing, spoofing, insider threats and DNS tunneling attacks.

DDoS attacks are **always** deliberate.

In the second half of 2023, DDoS attackers targeted:

Enterprises across all industries | Very large to very small companies | Airports, hospitals, utilities, and other critical infrastructure | Federal, state, and local governments – including schools | Telecom and cloud companies | Many more

And they attack organizations multiple times.

One example: in Q4 2023, Zayo mitigated **over 140 individual DDoS attacks** launched against a single consulting firm. The firm was protected by Zayo, so their business was unimpacted.

This report contains insights, analysis, and conclusions about each industry under attack. Further, it provides you the steps to take to ensure your business isn't harmed by the DDoS attacks heading your way.

Conclusion

DDoS attacks are here to stay. Year over year we're seeing growth in their frequency, length, and bandwidth power. Further, they're becoming more sophisticated, more automated, stealthier, and harder for attacked organizations to detect. DDoS Protection has largely kept pace, itself evolving to be able to protect organizations against attacks in real-time, and now, **proactively**.

Methodology

This report analyzed more than 103,000 threat detections and mitigations experienced by Zayo customers in 2023. The data, spanning 14 industries and regions across North America and Western Europe, covers the period from January 1 to December 31, 2023. Notably, 72,000 of these attacks occurred in the first half of 2023, and 31,000 occurred in the second half.

"Most people on the Internet aren't plotting a DDoS attack. But the Internet is a big place, and Dark Web crime is the fastest growing business on earth. **Attackers are leveraging sophisticated technologies and cutting edge techniques to** innovate the ways they **deceive**, **disrupt** and **destroy our most critical data.**"

- Eric O'Neill, National Security Strategist, Carbon Black

Table of Contents

Let's Begin

Welcome to Zayo's DDoS Insights Report for year end 2023.

This report reviews DDoS attack data collected from Zayo's network-based DDoS protected customers. Within this report, we illustrate who is being attacked, how frequently the attacks occur, when attacks occur, how long each attack lasts, and the size of the attacks.

The insights provided within this report illustrate the DDoS attack landscape across the businesses Zayo protects.

Ups and Downs - But Ultimately Up

For the customers Zayo protects, we've seen significant fluctuations in DDoS activity through 2023:

387% increase
in DDoS attacks
From Q1 to Q2

74% drop
in DDoS attacks
From Q2 to Q3

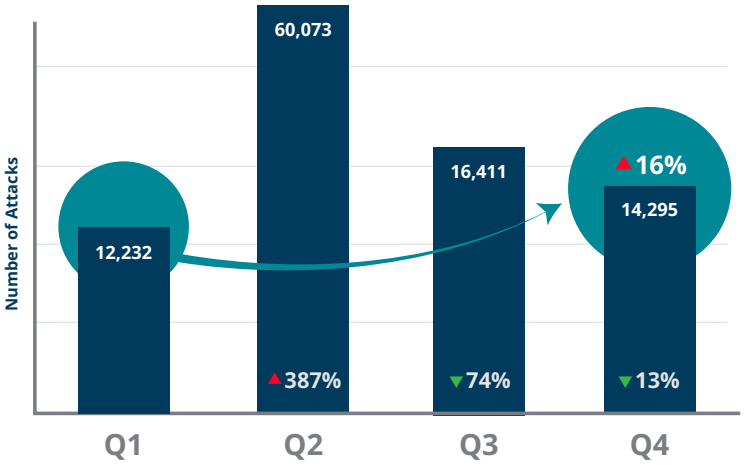
13% increase
in DDoS attacks
From Q3 to Q4

Comparing Q4 to Q1, 2023, there was a **16% increase** in attack activity across industries.

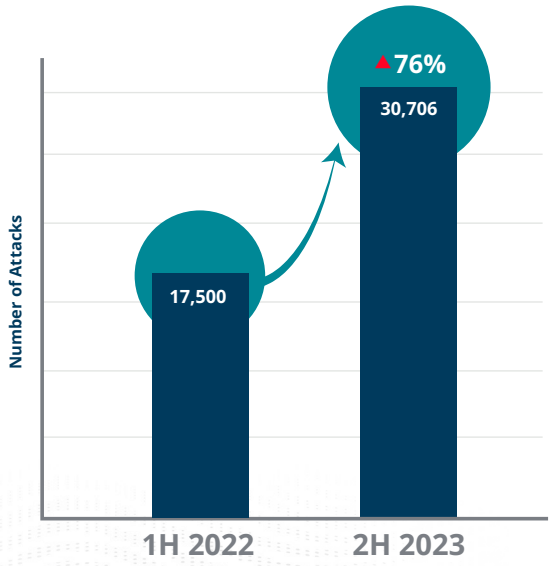
Past evidence and current environmental factors both point toward the inevitability of future increases in DDoS attacks in the years to come:

- Since early 2021, there has been a 150% increase in DDoS attacks globally.
- A new cyber attack occurs every 39 seconds.
- Some say there are approximately 23,000 DDoS attacks every day globally. Others claim over 40,000.
- DDoS attacks can be costly to any business, but unprotected businesses experience an average cost of $200K per attack. This too is rising.
- DDoS attack frequency rose 200% YoY from 1H22 to 1H23, and still managed to rise 76% from 1H22 to 2H23.

Number of Attacks Detected by Zayo Scrubbers (2023)



Number of Attacks Detected (Previous 24 Months)



It's easy to see why we're experiencing increasing attacks

These factors contribute to an environment easily exposed to DDoS attack attention:

- Our global landscape of increasing **digitization** (automating attacks while increasing points of vulnerability, so attacks are easier to pull off)
- Political **unrest** (making the outcome of attacks attractive to those carrying them out)
- The emergence of widespread adoption of **work-from-home** (vastly increasing the attack surface with thousands of new entry points)
- As always, **profit**, with attackers demanding a ransom to stop the attack

As attacks increase in number and frequency, they also grow in size, sophistication, and ultimately, success. When DDoS attacks are successful, businesses lose time, money, customers, and reputation.

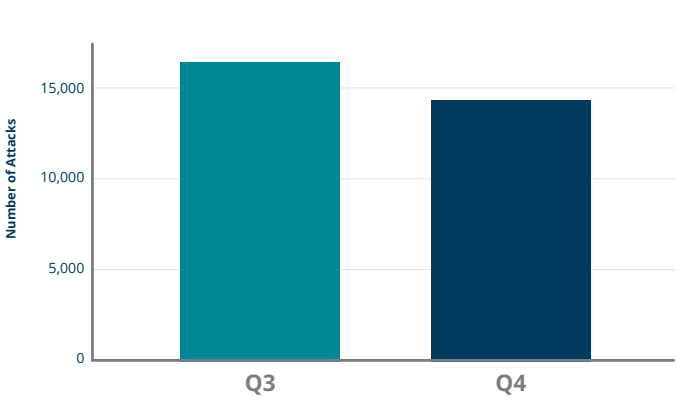
As a Tier-1 Internet provider, Zayo's DDoS Protection happens in the network. We provide DDoS defense that isn't dependent on appliances and doesn't require specialized skills. It's:

- Exceptionally responsive
- Always on, and protecting customers in the background
- Monitored by Zayo's Security Operations Center (SOC) around the clock

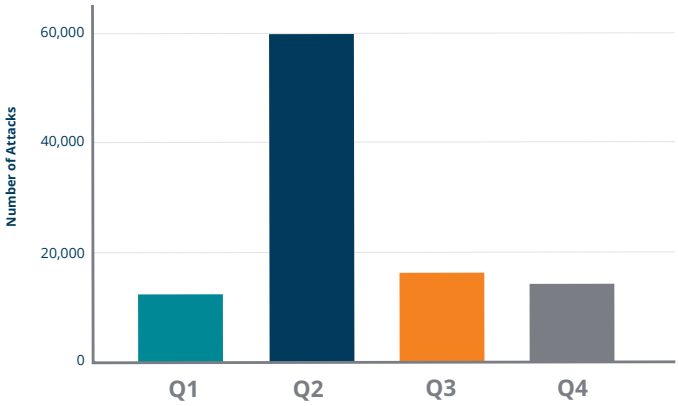
The Frequency of DDoS Attacks

Zayo consistently monitors the frequency of DDoS attacks across industries, and the comparison between Q3 and Q4 2023 reveals a consistent level of attack occurrences. **DDoS attacks aren't going away.**

Total Number of Attacks (2H 2023)



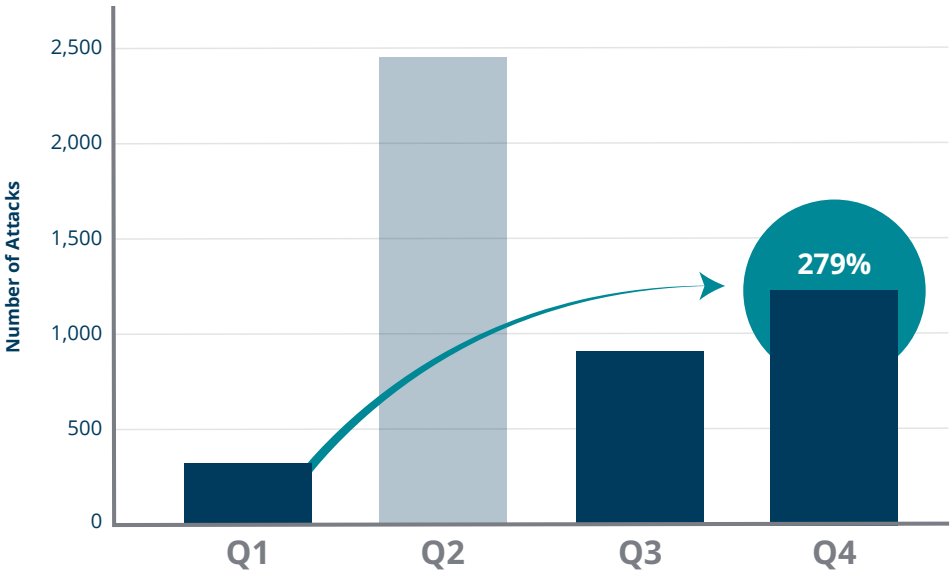
Total Number of Attacks (QoQ 2023)



Industries across the Zayo customer base consistently faced a high number of attacks throughout 2023. Specifically, during this period, the following industries witnessed a continuous quarter-over-quarter increase in DDoS attacks:

Manufacturing

Manufacturing Total Number of Attacks (QoQ 2023)

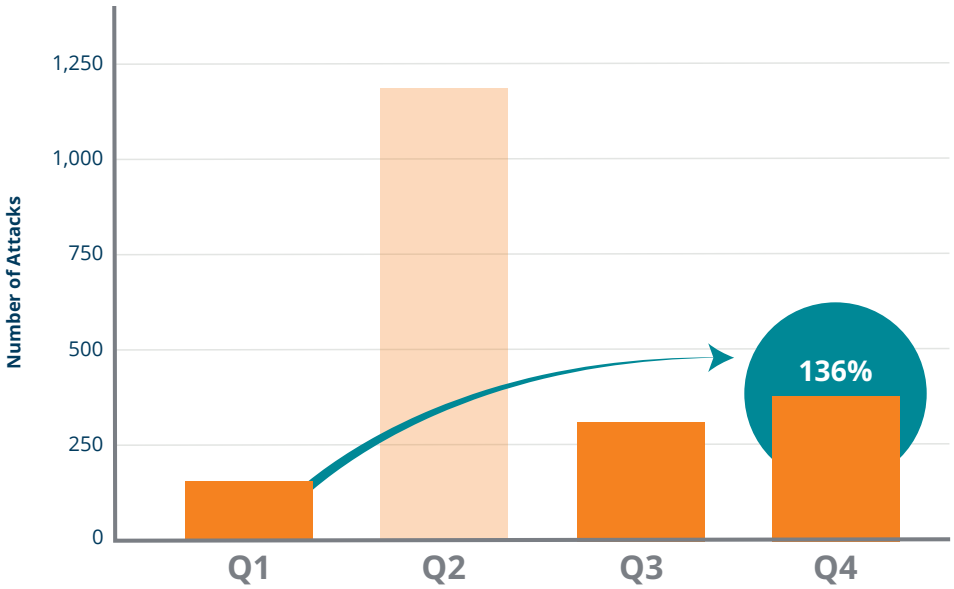


Starting at the beginning of the year and removing the Q2 spike, the Manufacturing sector saw an **increase of 279% in attack frequency** by the end of Q4.

Why? For one, we're seeing an on-shoring movement in the industry. U.S. manufacturing has undergone a revival with global supply chain shifts, reversing the trend of overseas relocation. And with movement come disruptions in production, leading to operational vulnerability. DDoS threats to manufacturing take advantage of these disruptions, as well as communication breakdowns between Operational Technology (OT) control systems and their Industrial Internet of Things (IIoT) devices.

Healthcare

Healthcare Total Number of Attacks (QoQ 2023)

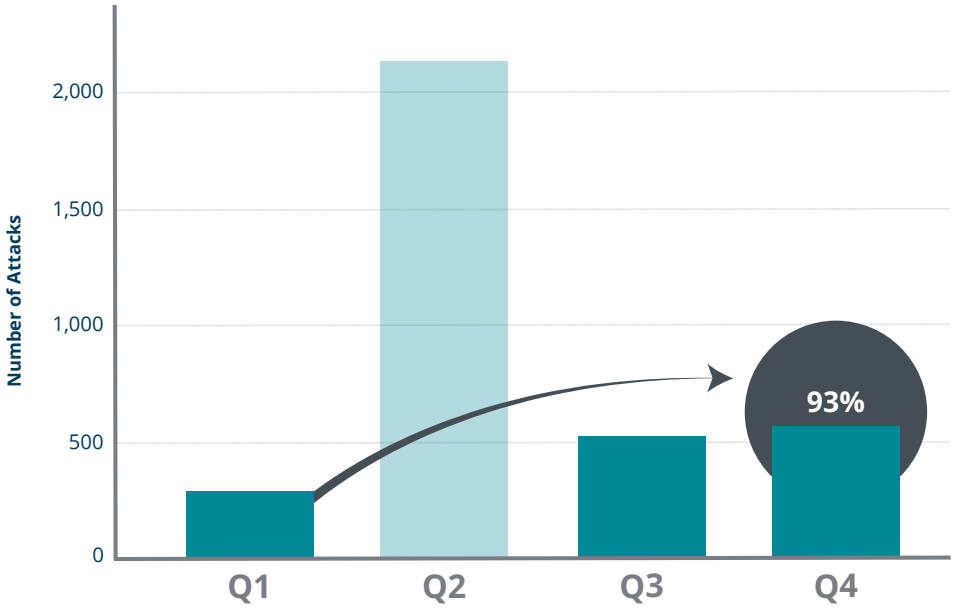


Healthcare continues to be a favorite target for DDoS attacks. DDoS attacks **increased 136%** from Q1 to Q4 2023. Healthcare continues its journey toward a full digital transformation. By 2027, healthcare companies will spend an estimated $974.5 billion on IT alone. DDoS attacks on healthcare aim to disrupt services, compromise patient data, or advance hacktivist agendas.

This sector must prioritize investing in security measures to safeguard both patients and digital assets.

Finance

Finance Total Number of Attacks (QoQ 2023)



The finance industry is a high-value target for DDoS attackers. While it's never easy to divine the motive of an attacker, these companies could offer attackers an opportunity for financial gain through extortion, operational disruption, chaos, market manipulation, theft of sensitive customer data, and the advancement of hacktivist agendas.

"Law firms are pretty far from being attractive victims for cybercriminals. However, their clients — namely, secrets of their clients — make law firms a magnet for all kinds of cybercriminals."

- Ilia Kolochenko, Chief Architect at application security firm ImmuniWeb. **Source**

Was Q2 2023 an Outlier?

Across industries and across every DDoS attack element measured, Q2 2023's DDoS profile was magnitudes higher than the previous, and following quarters.

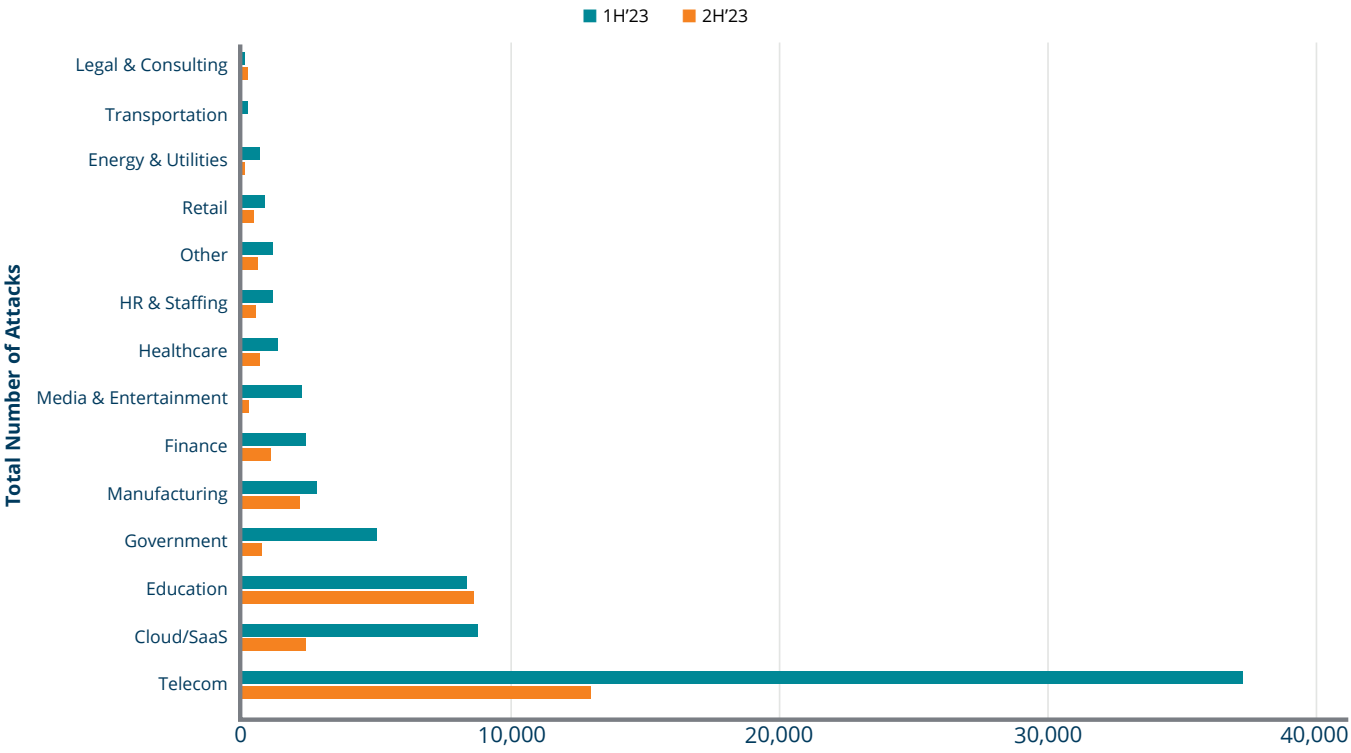
What happened in Q2 2023? A number of factors contributed to this spike:

- Killnet**.** Russia's invasion of Ukraine began in February 2023. Around March, Russia formed this pro-Russia DDoS hacker group in order to launch DDoS attacks toward government institutions and private companies of countries seen as pro-Ukraine. As reported by Mandiant, Killnet was responsible for over 500 large-scale attacks in the first half of 2023. Killnet's operations are shifting to a commercial, botnet-for-hire model, resulting in a (perhaps temporary) drop in attack volume.
- **Multi-vector attacks.** Multi-vector attacks are starting to replace volumetric attacks. Multi-vector attacks were larger in Q2, and are becoming more sophisticated, more targeted, and smaller, contributing to a drop in overall attack size in the second half of the year.
- **The burgeoning upswing of for-hire botnet usage:** we've seen an escalating reliance on botnets for attacks as industries increase their use of APIs, IoT, and other inadequately-secured digital infrastructure. Botnets contributed to the Q2 spike in attack activity. Operation PowerOFF seized 48 domains connected with DDoS-for-hire services, perhaps contributing to the drop in attack activity in Q3.

In the second half of 2023, DDoS activity resumed the steadily growing levels we saw before the second quarter's spike.

In 2023, the second quarter was an outlier. However, we expect similar erratic jumps in DDoS activity in future quarters as threat actors add newer technologies (such as AI) to their arsenal of attack tools, and as the world's political and economic landscape changes.

Total Number of Attacks Per Industry (1H 2023 vs 2H 2023)



The industries that experienced the most frequent attacks throughout 2023:

Telecommunications **49% of all attacks**

Telecom accounted for almost half of all the DDoS attacks in 2023 (51% in the first half of the year, 42% in the second). Threat actors are targeting Internet providers directly, with destructive impact to their operations and their customers.

A devastating second quarter across all industries was especially bad for telecom. This industry was attacked 1,175% more in Q2 than in Q1. Why Telecom?

- **The prize of sensitive information belonging to millions of users**
- **The possibility of disrupting communication for political purposes**
- **The vast attack surface of their (often outdated) digital assets**

Whatever the motive and means, telecom is clearly not immune to DDoS attack disruption.

Education 17% of all attacks

The ease and affordability of botnet-for-hire services, combined with frequent gaps in the cybersecurity of educational institutions, make education an easy target.

"Fully 17% of all DDoS attacks targeted educational institutions. A DDoS attack on education not only disrupts the pursuit of knowledge, but often shuts down operations and can cost institutions a lot of money. DDoS attacks can also serve as distractions, tying up limited resources and introducing vulnerabilities to other cybercrimes that represent even greater safety threats for our students."

- Gayle Nelson, VP, Education Sales, Zayo

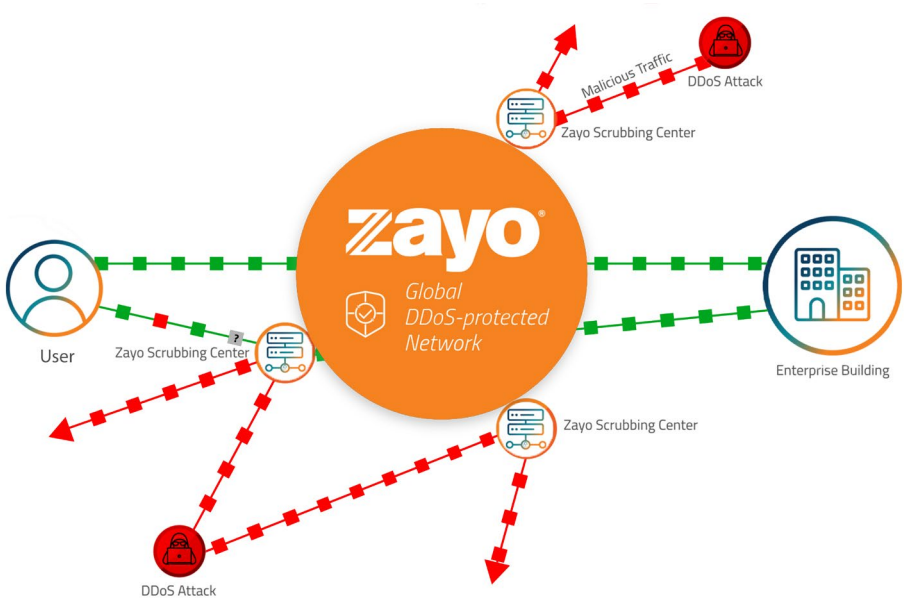
Cloud/SaaS 11% of all attacks

Why do attackers target Cloud and SaaS providers with such frequency? First, attackers can cause widespread damage to cloud and SaaS providers' intricately interconnected core infrastructures. A quick ransom payment stops the attack. Attackers could also be fishing for vulnerabilities - searching for security weaknesses where they can target larger attacks later.

DDoS Protection is Everyone's Force Field:

If your business is protected, the number of attacks directed toward you doesn't matter. With automated DDoS Protection from Zayo, none of the attacks will reach your network, leaving your online traffic flowing as usual and your business operations impervious to the attack.

Zayo has taken a unique approach. A single DDoS subscription immediately protects all of your IP addresses across your whole network, rather than paying on a per-circuit basis. This aggregate protection **costs less** and **scales based on your usage**.



We analyze, redirect and scrub **each individual IP address** attacked, without the collateral damage of latency caused by touching your healthy traffic.

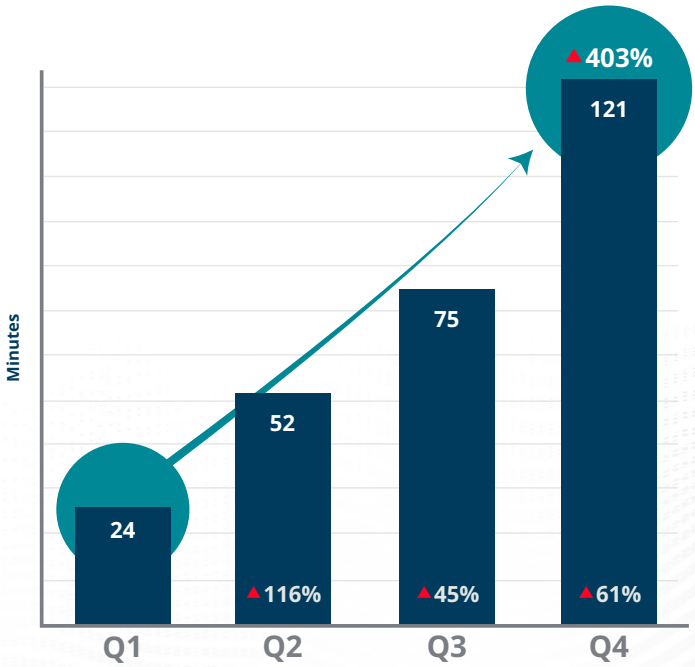
The Duration of DDoS Attacks

In the second half of 2023, short burst attacks – those lasting less than 10 minutes – still represent the vast majority of attacks.

Specifically, **over 72% of all attacks during this period were of this short duration**. However, this percentage represents a decrease from the first half of the year, when 83% of attacks were under 10 minutes in length.

This represents a **worrying trend**. As attack frequency has dropped, attack duration has lengthened. Overall, attacks are more sustained, lasting much longer:

How Long Do Average Attacks Last? (QoQ 2023)

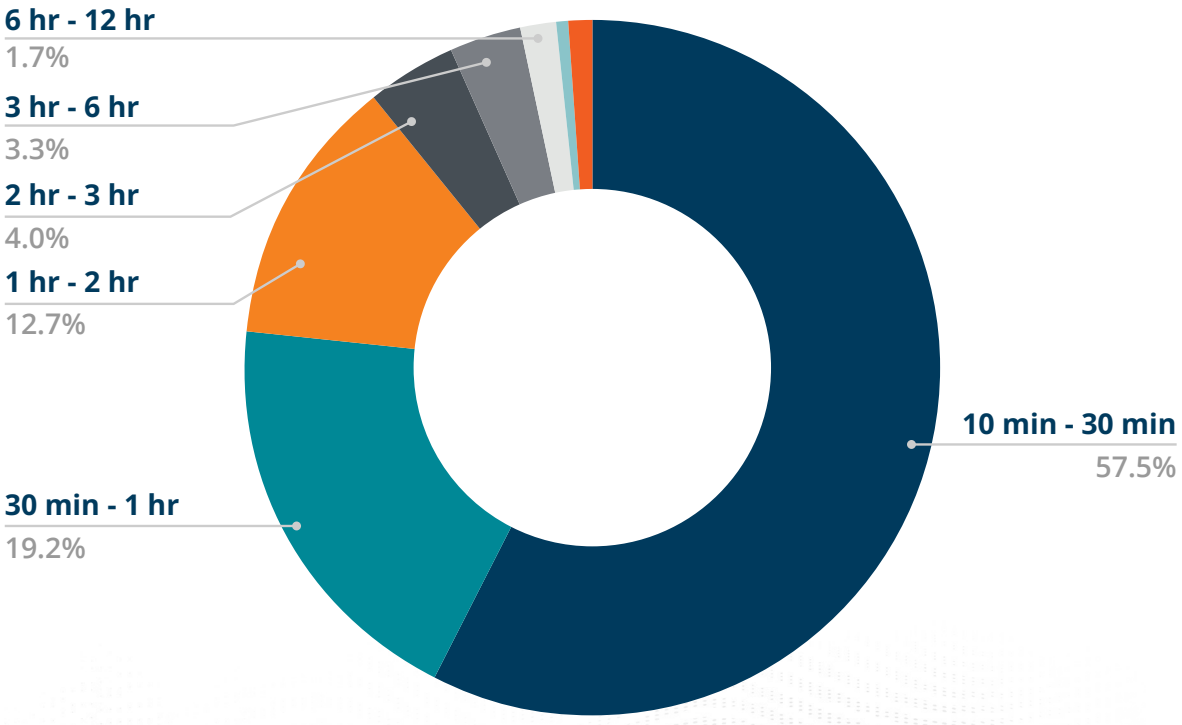


First, Why So Many Short Attacks?

Most attacks start and stop in under 10 minutes because:

1. Short attacks can be used as **feelers** – areas of vulnerability in the targeted business. Attackers can strike with a larger attack when they find weaknesses in cybersecurity defenses.
2. Short attacks are **efficient**. Companies, schools, government agencies and other organizations can shut down for an entire day with just a few minutes of network disruption.
3. Attackers will see that an organization is **protected** and stop the attack, creating a data set of shorter attacks. Attackers may have intended the short attacks to be longer ones.

Distribution of Attacks Over 10 Minutes (2H2023)



While even short attacks impact the victim's operations, the longer the attack, the more significant the impact. If an attack gets through, its duration can expose an attacker's intent. Exactly how disruptive does the attacker want the attack to be?

The duration of an attack has a real impact on an unprotected business:

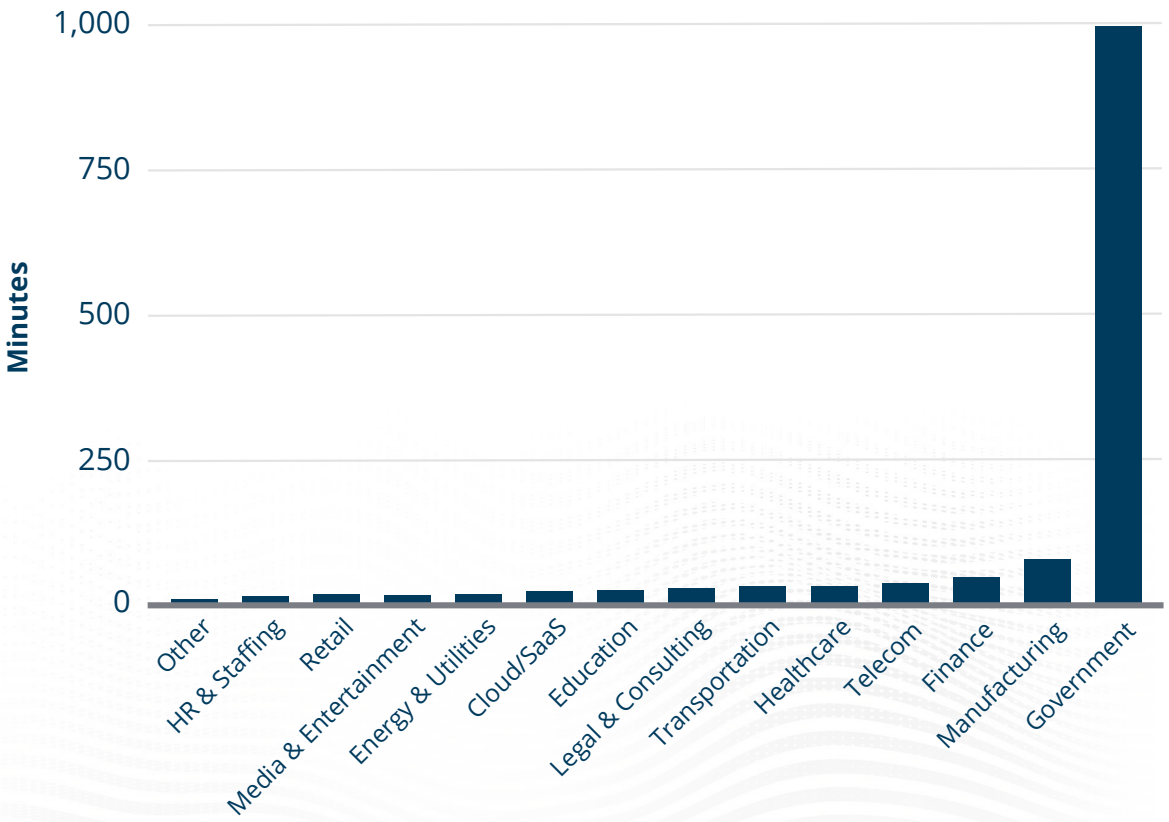
Customer experience:
Customers can't interact with you if they can't connect to your network. Downtime hurts your reputation and hinders future business.

Employee experience:
Employees can't work remotely or in an office if they are not connected to your network. How long can you afford to be offline?

Financial impact:
What is the cost of fixing the network? Of regaining lost business? Of paying a ransom to the attacker? Of mending a damaged reputation?

The longest attack in 2H lasted for **17 days**, 2 hours, 36 minutes, 55 seconds. Even when attacks last for weeks, **protected businesses are unimpacted**.

Average Duration of Attack by Industry (2H 2023)



Sustained Attacks Against Government on the Rise

In the first half of 2023, government entities experienced the longest attacks with an average attack time of four hours and 20 minutes.

In the second half, government entities continued to experience the longest attacks of all industries observed. But in the second half, attack duration swelled to **nearly 18 hours** per attack on average. This represents:

- A **322% increase** from the first half
- A **1,141% increase from the beginning to the end of 2023**

Why are government entities attacked with such persistence?

Political unrest:
Government organizations are often targeted by attackers with political motivations or grievances. These attackers may have a specific agenda and are willing to invest significant time and resources to achieve their objectives. We can expect federal, state and local government institutions to continue the need to battle these sustained attacks during this 2024 presidential election year.

Complex infrastructure:
Government networks and systems are often complex and distributed, making them more challenging to defend against attacks. The larger the infrastructure, the more time it takes to detect and mitigate DDoS attacks, making them last longer.

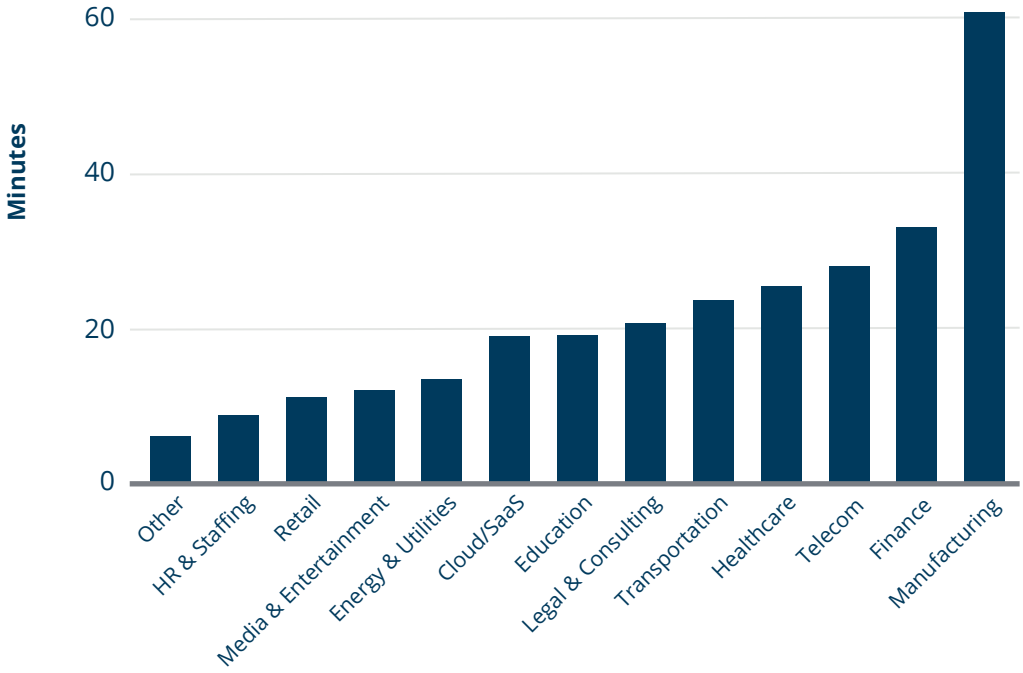
High stakes:
Government services often provide critical services to citizens, making them high-value targets for attackers seeking to cause disruption and chaos. Attackers know that even a brief disruption of government services can have significant consequences, which motivates them to launch long-lasting and persistent attacks.

Across all industries, the average **duration of attacks in 2H2023 increased by 158%** from the first half of the year.
Across all industries, attacks in the fourth quarter were **403% longer** when compared to the first quarter.

Manufacturing, a New Favorite Target

In the second half of the year, **manufacturing** replaced healthcare as the victim of the second-longest average attacks, at over 1 hour per attack. Manufacturing's processes are increasingly digitized, and their own supply chains increasingly connected. The second half of the year is an especially busy time for production - expanding the sector's attack surface.

Average Duration of Attacks - All Industries, excluding government (2H2023)



"A DDoS attack on manufacturing **disrupts more than production lines**; it disrupts entire supply chains, and it brings to light the vulnerability of global interconnectedness. As on-shoring gains momentum, protecting against DDoS attacks ensures that your network is stronger than the digital attacks it faces."

- Nias Battle, VP, Business and Consumer Services Sales, Zayo

And once again, **finance** companies experienced longer-than-average attacks as well, at over 30 minutes per attack.

Finance institutions have highly valued and sensitive information that proves irresistible for attackers seeking identity theft or financial fraud. Attackers may be more persistent in their efforts to extract data or cause disruption, leading to more prolonged DDoS attacks.

Aside from manufacturing and finance, the industries whose average attack duration increased the most from Q1 to Q4 2023 were:

- **Education** (23 minutes per attack - a **206% increase**)
- **Media and Entertainment** (16 minutes per attack - a **111% increase**)
- **Telecommunications** (33 minutes per attack - a **104% increase**)

Other notables:

- **Cloud & SaaS** companies experiences an **increased attack duration of nearly 350%** from Q2 to Q3, and another 11% from Q3 to Q4
- **Healthcare** companies experienced a **158% increase** in attack length from Q2 to Q3.

Across all industries, average attack duration increased 138% from 1H to 2H, and 403% when we compared Q4 to Q1.

"A 30-second spurt attack would lead to a full hour loss"

- Billy Russell, Technology Director at North Judson-San Pierre Schools in North Judson, Indiana

Protect Your Business

You can shorten the duration of an attack (indeed, make it nearly **imperceptible**) with an automated redirect of attack traffic from your network ingress to scrubbers that will ensure only legitimate traffic passes.

With automated DDoS Protection, attack length does not matter. An attack of hours – or even weeks – would have zero impact on a protected business.

The truth of the matter is that being a digital business exposes you to network risks. Every business in every industry has confidential information to protect.

DDoS attacks can occur in the background, quietly disrupting your business while you remain largely unaware. According to IBM, it takes a company 197 days to discover a breach and up to 69 days to contain it. Companies that contained a breach in fewer than 30 days saved more than $1 million compared to those that took more than 30 days.

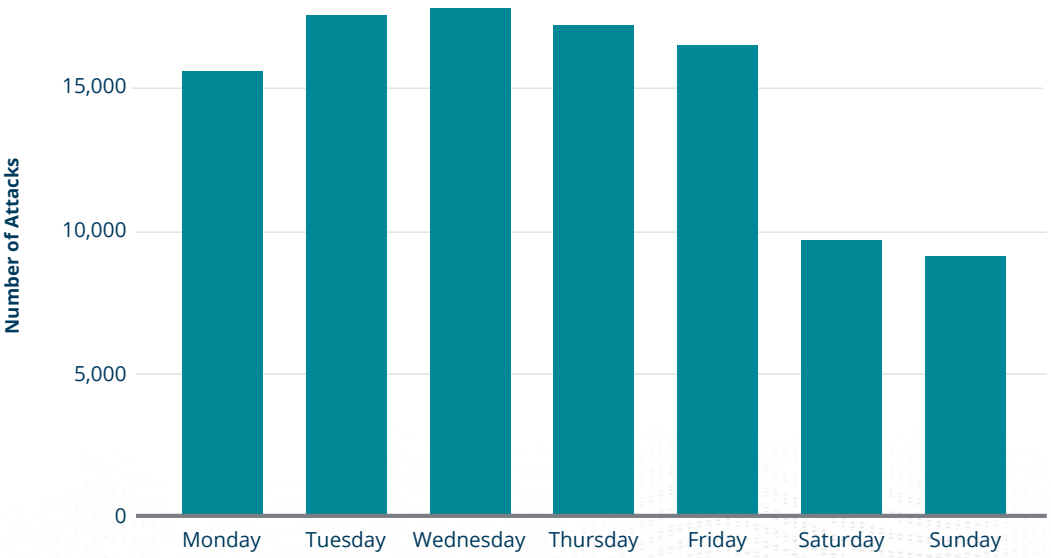
DDoS Protection can't stop DDoS attacks, but will stop them from impacting your business.

The Time of DDoS Attacks

When can you expect an attack? **The timing is strategic.**

Similar to the first half of 2023, attacks in the second half also occurred during the most disruptive times – within the business week and specifically during business hours. Even hackers from overseas synchronize their attacks to coincide with the busiest periods of the business day when your network is crucial for both employees and customers.

When Attacks Occurred During the Week (2023)

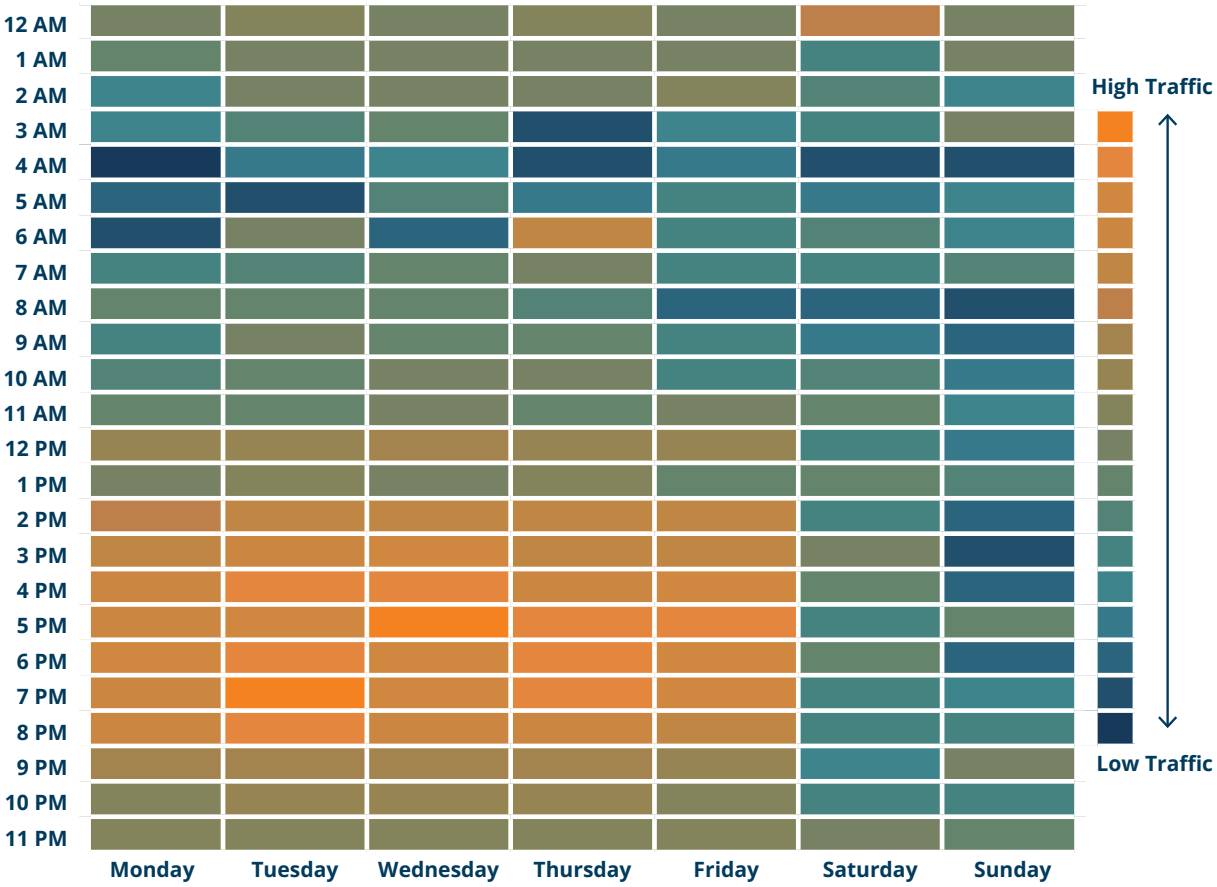


The middle of the work week saw the most traffic. **57% of attacks** in 2023 happened on a **Tuesday and Wednesday**.

The timing of attacks in Q3 and Q4 mirrored those in Q1 and Q2.

Attacks occurred most consistently during the U.S. business day. Yet, with continuous online presence, consumer activity on the Internet may lead to outlier attacks occurring beyond the usual business hours.

When Attacks Occurred During the Day, Eastern Time (Q3 and Q4, 2023)



The timing of attacks in Q3 and Q4 mirrored those in Q1 and Q2. Attacks occurred most consistently during the U.S. business day. Yet, with continuous online presence, consumer activity on the Internet may lead to outlier attacks occurring beyond the usual business hours.

Zayo is proactive. We **monitor** your network to establish normal traffic patterns, **identify** malicious traffic at the onset, and **protect** you during an attack, ensuring only legitimate traffic passes through. After the attack is over, and traffic has remained clean, Zayo will **restore** traffic to its original path.

The Size of DDoS Attacks

How big will this battle be?

Like frequency and duration, the size of a DDoS attack (measured by the amount of bandwidth used by the attack) can affect how long it takes to stop it and how damaging its effects are to your organization.

Like in the first half of the year, retail organizations continued to face the largest DDoS attacks, with healthcare companies following. Customers in these two industries experienced the weightiest attacks on average, while the top 10% of attacks by size continued to focus on telecom.

Average Attack Size per Industry (Gbps)

Industry	1H2023	2H2023	Δ
Retail	3.1	2.9	▼8.0%
Healthcare	2.2	1.8	▼18.2%
Telecom	3.0	1.7	▼42.8%
Energy & Utilities	2.4	1.7	▼28.5%
Manufacturing	2.2	1.7	▼24.5%
Government	1.9	1.4	▼24.2%
Media & Entertainment	3.5	1.3	▼62.6%
Legal & Consulting	0.6	1.3	▲117%
Cloud/SaaS	2.0	0.9	▼56.8%
Transportation	0.8	0.9	▲17.4%
Finance	1.3	0.7	▼49.6%
Education	0.7	0.4	▼36.1%
Other	0.5	0.4	▼17.9%
HR & Staffing	2.4	0.0	▼100.0%
Average	**1.9**	**1.3**	▼33.1%

It should be noted that Zayo did not see the increase in size of attacks other organizations are reporting.

Notably, across all industries, the overall size of DDoS attacks detected by Zayo dropped, by a lot, from the first half to the second half of 2023. The average attack in the first half of the year was 1.9 Gbps, dropping to an average of 1.3 Gbps in the second half of the year.

This is not the good news story it seems to be

This 33% decrease in attack size is a symptom of a larger disturbing trend. Volumetric type attacks are declining. Volumetric attacks are typically the largest and most visible attacks, the ones that are easiest to mitigate because they're easiest to spot.

However, **they're being replaced by "multi-vector" attacks**. If we think of a "vector" as a means of entry to your systems or network, a multi-vector attack spreads its destructive power more widely (albeit: thinly), targeting individual IP addresses, email systems, databases, or web browsers with just a few megabytes of probing traffic. These "feeler" attacks are much harder to detect.

Multi-vector attacks can employ the following attack types simultaneously:

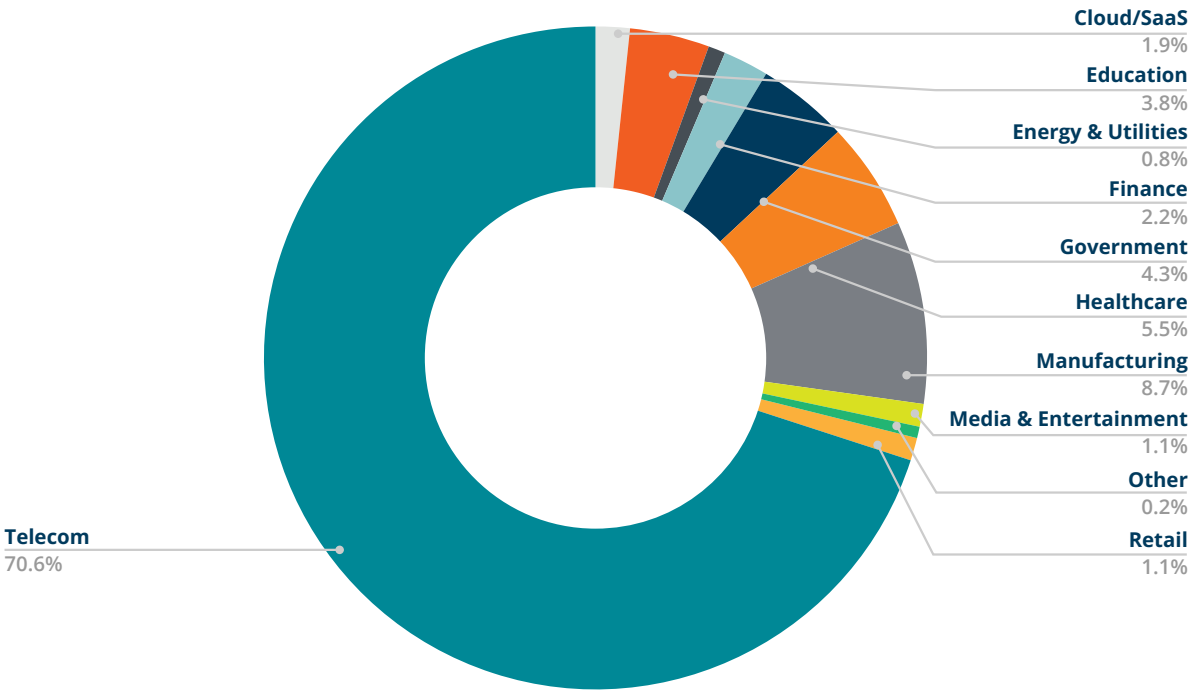
- Carpet-bombing attacks, where the attacker targets its malicious traffic from multiple sources toward multiple targets simultaneously
- DNS water torture attacks, also known as DNS flood attacks, where the attacker targets the DNS infrastructure, usually with a botnet-generated flood of requests
- TCP attacks, where the attacker searches for vulnerabilities or weaknesses in the TCP protocol stack and exhausts the server's resources or disrupts the TCP communication path between clients and the server
- HTTP/HTTPS attacks, achieved by flooding the server with a massive volume of HTTP requests, such as GET or POST requests, consuming bandwidth, processing power, and memory

This **33% decrease** in attack size is symptom of a larger disturbing trend. Large attacks are being replaced by multi-vector attacks.

Massive DDoS Attacks Still Overwhelm

Two industries, **transportation** and **legal & consulting**, suffered larger attacks in the second half of the year compared to the first. Interestingly, these same two industries also experienced the greatest increase in attack frequency from Q3 to Q4, 2023 (a 186% increase for legal & consulting, and a 225% increase for transportation).

Of the Largest 10% of Attacks, Here's Who Was Targeted



Further analyzing attack size, we took the top 10% of all attacks by bandwidth - 3,053 of the largest attacks - and saw that the top five industries facing the brunt of these especially large attacks were telecommunications, manufacturing, healthcare, government and education organizations.

Industry	1H'23	2H'23	Δ
Telecommunications	73.7%	70.6%	▼4%
Manufacturing	2.6%	8.6%	▲231%
Healthcare	2.3%	5.5%	▲139%
Government	5.1%	4.3%	▼16%
Education	1.3%	3.8%	▲192%

Why did attackers direct their largest attacks toward these industries?

Usually, the larger the target, the larger the brute force needs to be to match the size of the server traffic running applications. Large scale attacks are also easy to launch; since servers don't allocate resources to applications equally, attacking a single server resource heavily can take the whole server down.

Telecommunications (1.7 Gbps average attack size)

Telecommunications companies are the source of the Internet. They provide the bandwidth all companies rely on to reach their customers. If an attacker can cripple a telecommunication company, the effect ripples through the information chain, impacting thousands of users, with a significant overall impact.

Manufacturing (1.7 Gbps average attack size)

A combination of business and networking practices have made manufacturing an increasingly valuable target for cyber attacks. Manufacturers have a broad digital supply chain and often connect to their partners using APIs. Additionally, they've adopted, perhaps more than other industries, IoT, robotics and AI within their facilities. Each digital connection exposes manufacturers to potential vulnerability. And the second half of any year ramps up production in preparation for the holiday season - a prime time for ransom-motivated attacks.

Healthcare (1.8 Gbps average attack size)

In 2023, the Department of Health and Human Services (HHS) division of cybersecurity reported 568 separate instances of cybercrime directed toward healthcare organizations. Most of these incidents reported hacking, unauthorized access, theft and loss. Further, the Russian Killnet DDoS attacks that occurred earlier in the year - attacks that so disrupted the healthcare industry - are evolving into a new attack-for-hire service.

What motivates attackers to disrupt healthcare organizations, especially with such large attacks? A large DDoS attack is a major obstruction to patient care, and is often used to distract a security organization while the attacker feels for vulnerabilities and plots a larger theft. Sensitive patient data is valuable. As discussed earlier, ransom attacks are especially prevalent in healthcare, and the growing use of Electronic Health Records (EHRs) and other digital technologies has rendered the healthcare industry more exposed to DDoS attacks.

Government (1.5 Gbps average attack size)

Government dropped from the list of the top five sectors attacked with the most frequency, but remains among the top five targeted with these largest attacks.

The size of DDoS attacks against government entities has exponentially grown. In 2008, the largest DDoS attacks were a few tens of megabits per second. By 2016, DDoS attacks had grown to hundreds of megabits per second. Today, they've reached the next order-of-magnitude milestone of gigabits per second. The Department of Homeland Security (DHS) worries about agencies' continued ability to withstand such large repeated attacks.

The jump in number and size of attacks from Q1 to Q4 2023, showed the tactical shift toward automation. As Microsoft reported, tens of thousands of virtual machines can simultaneously launch an attack (the "distributed" part of DDoS). This automated ease, coupled with the potentially large payout of public sector disruption, can explain a jump in attack size targeting the government.

Education ranked fifth on this list - they were the target of nearly 4% of the largest 10% of attacks detected and mitigated by Zayo. This is a big jump from the first half of the year, and it makes sense.

"The sheer number of DDoS attacks against government entities serves as a stark reminder of the ongoing battle to defend our democratic institutions from digital chaos. **2024 brings no shortage of political unrest**, and a presidential election will draw the attention of attackers against municipal, local, and federal government targets. Enhanced protection is critical and Zayo plays a key role in delivering that protection."

- Jason Taylor, VP, Government Sales, Zayo

Education (410 Mbps average attack size)

DDoS attacks are easier than ever to implement and launch. With little cyber knowledge or expertise, almost anyone can find a way to purchase a DDoS attack online, inexpensively. And schools are especially vulnerable; whether instruction is remote or in person, a single attack can disrupt an entire day of education.

The largest attack Zayo saw in Q3 2023 was a **404 Gbps** attack directed toward a **telecommunications company**. In Q4 2023, the largest attack was 399 Gbps - whose target was the same company. A large attack aimed at the source of online communications can impact the thousands of companies using that service.

The Future of DDoS Attacks

Automation has Taken Hold

2023 showed us what exponential growth in DDoS activity looks like. Bot-based attacks have made it easier to attack more frequently, in a more sustained manner, with more requests per second. The next evolutionary step will be a new level of intelligence in attacks - DDoS attacks that leverage AI to overcome defenses in a more surgical manner.

DDoS Protection is rising to the occasion.

"Bring Any Site Down for as Low as $1/day!"

So advertises PaperStressor ("2023's Best DDoS Tool!"). Thinly disguised as a stress-test for your own network vulnerability, it's a bot, ready to launch an attack against, well, any target a $30/month subscriber would like. A barrier to cybercrime entry that's so low that almost anyone - a student who didn't study for a test, for example - can purchase and launch.

Organizations of All Sizes

In many ways, the smaller the business, the more vulnerable. Small companies generally have limited resources and weaker security measures than larger organizations, making them easier targets for attackers looking to test their mettle. DDoS attacks disrupt business operations, causing financial losses, brand reputation damage, and customer loss.

The cost of exposure far outweighs the cost of protection. Companies of all sizes, but especially those with limited in-house expertise, should invest in DDoS mitigation services and create a response plan to protect themselves.

It's Inevitable

We protect thousands of companies from DDoS attacks, so we know when and where attacks occur, how long they last, and who's being attacked most. Utilizing our extensive network and DDoS Protection data, we decipher the underlying narrative within the data, presenting our informed conclusions for your consideration.

"It's not hard to see that a key security trend coming up in 2024 - one that is going to adversely affect our customers - **is the rapid rise in DDoS attacks.**"

- Anna Claibourne, Senior VP of Packet and Product Software, Zayo

Will you be attacked?

Yes.

DDoS attacks are increasing in frequency, duration, size, automation, sophistication, and therefore, **inevitability**. It's a profitable model for attackers, so, big or small, expect your business to be targeted one day.

Zayo protected our customers from an average of nearly **170 DDoS attacks per day** in the second half of 2023.

Why will you be attacked?

It depends.

Attackers have their own agendas:

- To discover vulnerabilities in an organization's online security
- To distract while the attacker captures confidential information
- To debilitate or damage the reputation of a company
- To extort a ransom to stop the attack
- To exact revenge, to make a political statement, or simply to troll
- To cover up secondary style attacks such as extortion or data theft

2024 is a federal election year in the United States. We expect an increase of attack activity, from both domestic and global sources to target government, education, and critical infrastructure.

What does a DDoS attack do?

It inflicts digital chaos.

Your customers, staff, and associates can no longer access your information online. Your website isn't responding. Your files aren't loading. Your customers are receiving error notices. Your business stands still.

Time to Exhale

We've provided a dire DDoS attack outlook in this report.

But know that **Zayo stays one step ahead**. With Zayo's network-based DDoS Protection service, you can protect your online presence, data, and customers from DDoS attacks.

Zayo stops DDoS attack traffic **before** it reaches your network and impacts your business.

Our DDoS Protection service is network-based, so you can put our network to work for you. A single DDoS Protection subscription from Zayo will stop any DDoS attack aimed at any of your IP addresses. Learn more about the uniqueness of our service in our DDoS Ebook.

The relative investment in DDoS Protection is tiny compared with the inevitable cost of DDoS attacks.

From Real-Time to Proactive

Zayo's DDoS Protection service already operated in real-time, automatically preventing the effects of an attack from impacting the targeted business.

Now, we're **proactively** protecting our customers, preventing attacks from occurring in the first place.

We've enhanced our DDoS Protection with a new **Intelligence Feed**. With this enhancement, we dynamically ingest data of DDoS attacks occurring worldwide, identify the source IP addresses, and then automatically block traffic from those malicious source IPs.

It's proactive.

It's adaptive.

It stops attacks before they start.

In today's digital landscape, the stakes have never been higher.

Protecting your organization from DDoS attacks isn't just an option; it's a critical necessity to safeguard your operations, reputation, and bottom line.

"We're in an attackers' market - very fertile soil for undetected cyber criminal activity. To stop the attackers from gaining the upper hand, we need DDoS protection that is as easy and effective as turning a switch."

- Eric O'Neill, National Security Strategist, Carbon Black

Secure Your Business With Zayo Today

Learn more about protecting your business from a DDoS attack.

Contact us for immediate support.