Protecting Your Business From Cyber Attacks

The State of DDoS Attacks

DDoS Insights From Q1 & Q2, 2023

zayo

Executive Summary

Q2 2023 saw an astounding **387% increase** in DDoS attack activity over Q1:

Telecommunications companies experienced the most **frequent attacks**, constituting ~50% of total attack volume with over **37,000** attacks in the first half of 2023

Yet, across all industries, companies saw a nearly **400% jump** in attack activity in the same timeframe.

The Government sector experienced the **longest attacks**, with an average attack lasting over **4 hours**

Yet, across all industries, the average duration of attacks **increased by 216%** in just one quarter, and even the shortest attacks can take a business offline for a full day.

Retail, Telecommunications, and Media companies experienced the **largest attacks**, with an average attack size of **3 Gbps** across all three verticals

Yet, across all industries, we've mitigated attacks ranging from **980 Gbps** down to just a few megabits, and even the smallest attacks can cause a business reputational harm.

Across all measures - it's getting worse, fast.

The Cost of Exposure: No matter the attack frequency, duration, or size, unprotected organizations experienced an average cost of $200,000 per DDoS attack.

Even small businesses are hit hard - it costs them $120,000 to recover from an average DDoS attack.

DDoS 101

A Distributed Denial of Service (DDoS) attack is a deliberate cyberattack against an organization's online presence. A DDoS attack floods a victim's Internet circuit with fake or illegitimate traffic to prevent true user traffic from passing. DDoS attacks are the most common type of cyberattack.

DDoS attacks are **always** deliberate.

In the first 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**
- **The telecom and cloud companies**
- **Many more**

And they attack vulnerable organizations multiple times.

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

Methodology

This report analyzes more than 70,000 threat detections and mitigations experienced by Zayo customers across 14 industries and regionally across North America and Western Europe between January 1 and June 30, 2023. Year-over-year comparative analyses refer to Zayo data collected during the same time frame from 2022.

Table of Contents

Let's Begin

Welcome to Zayo's DDoS insights report for Q1 and Q2 of 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.

DDoS attack frequency rose **200%** YoY.

The Grim Truth

Since early 2020, there has been a **150% increase in DDoS attacks globally**. A new cyber attack occurs **every 39 seconds**.

There are approximately **23,000 DDoS attacks** every day globally.

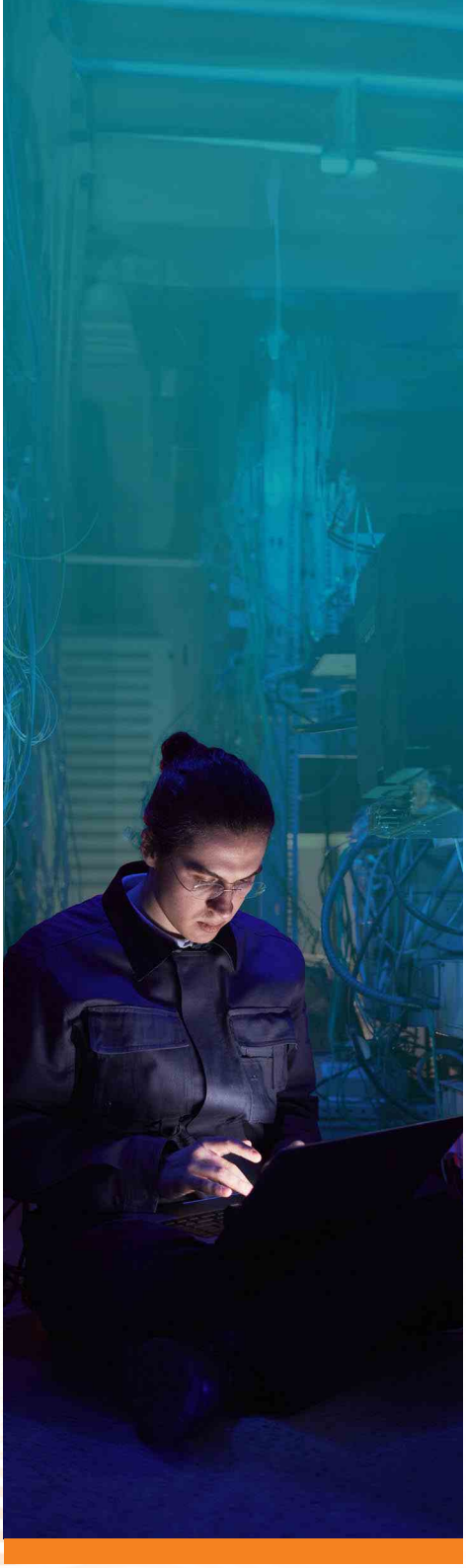
DDoS attacks can be costly to any business, but unprotected businesses experience an average cost of **$200K per attack**.

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**
- **Monitored by Zayo's Security Operations Center (SOC) around the clock**

Our global landscape of increasing digitization, political unrest, and the emergence of widespread adoption of work-from-home all contribute to an environment exposed to DDoS attack attention.

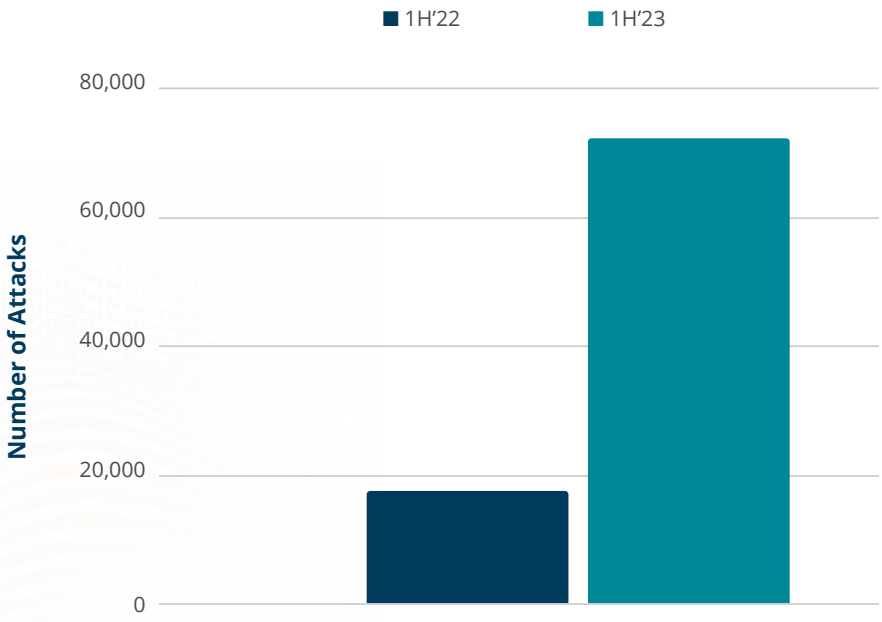
As attacks increase in number and frequency, they also grow in size, sophistication, and ultimately, success. When DDoS attacks are successful, businesses lose time, money, customers, and reputation.



The Frequency of DDoS Attacks

Zayo tracks how frequently DDoS attacks occur across industries. Comparing the first half of 2022 to the first half of 2023, we found that **DDoS attack frequency across all industries increased by 314%**.

Total Number of Attacks



While all industries are being attacked more, these industries in particular saw the most substantial increases in DDoS attacks during this time period:

Manufacturing

1,397% increase

Manufacturing is a critical infrastructure sector that relies on digital technologies, making it a target for DDoS attacks. Attacks disrupt production, damage reputation, and lead to financial losses. This increase in DDoS attacks was likely due to the sector's accelerating digitization and adoption of Internet of Things (IoT) devices, making it a more accessible target for hackers.

Media & Entertainment

1,065% increase

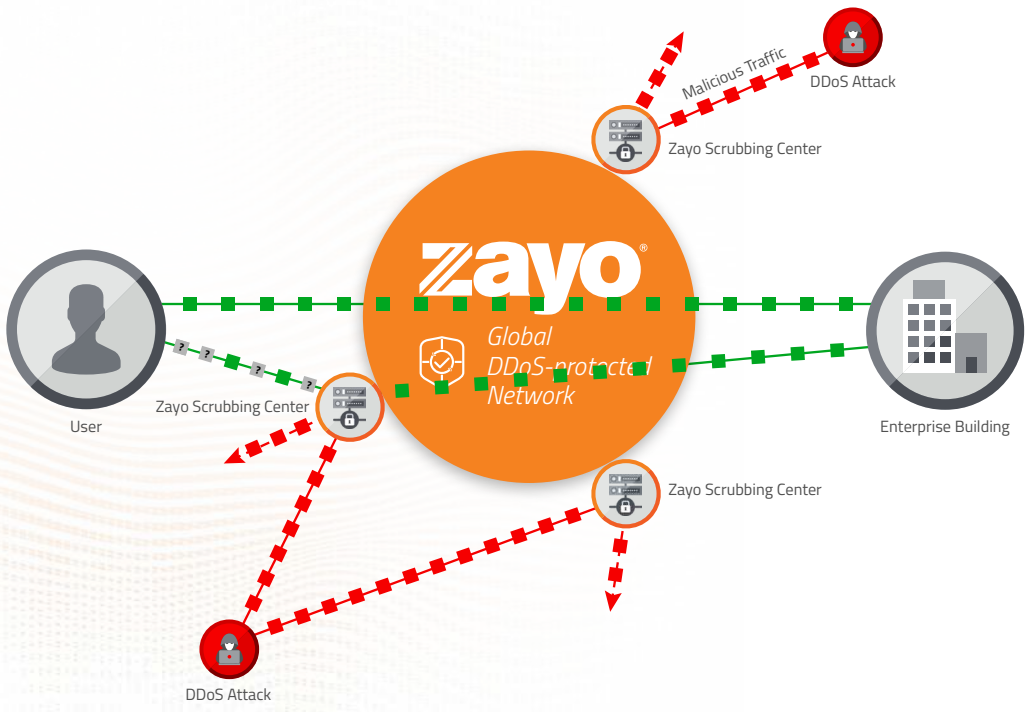
The sensitive intellectual property of media and entertainment companies are attractive targets. And since streaming is here to stay, their large online presence increases their attack surface. A perfect extortion target.

Cloud/SaaS

794% increase

Cloud and SaaS companies manage intricately interconnected online infrastructures. As a result, DDoS attacks have the potential to cause widespread impact on their clients, disrupting critical digital access.

Zayo analyzes, redirects, and scrubs **each individual IP address** attacked, without the "collateral damage" of latency caused by touching your healthy traffic.



A U.S. medical trauma center was caught off-guard by a DDoS attack. It disrupted their IP space, disabled their Electronic Medical Records (EMR), and shut down operations. Every patient, no matter the need, had to be turned away. Read about it here.

Healthcare

253% increase

Attackers can employ DDoS attacks to disrupt patient care, steal sensitive patient data, and cause financial losses. Ransom attacks are especially prevalent in healthcare. The growing utilization of Electronic Health Records (EHRs) and other digital technologies has rendered the healthcare industry more susceptible to DDoS attacks.

Finance

230% increase

The finance industry is a high-value target for DDoS attacks, where attackers such as Killnet can disrupt trading, prevent customers from accessing their accounts, and cause financial losses. As the steward of invaluable financial data, the finance industry's susceptibility is heightened by the proliferation of online banking and trading, which expands its digital presence and renders it most vulnerable.

Government

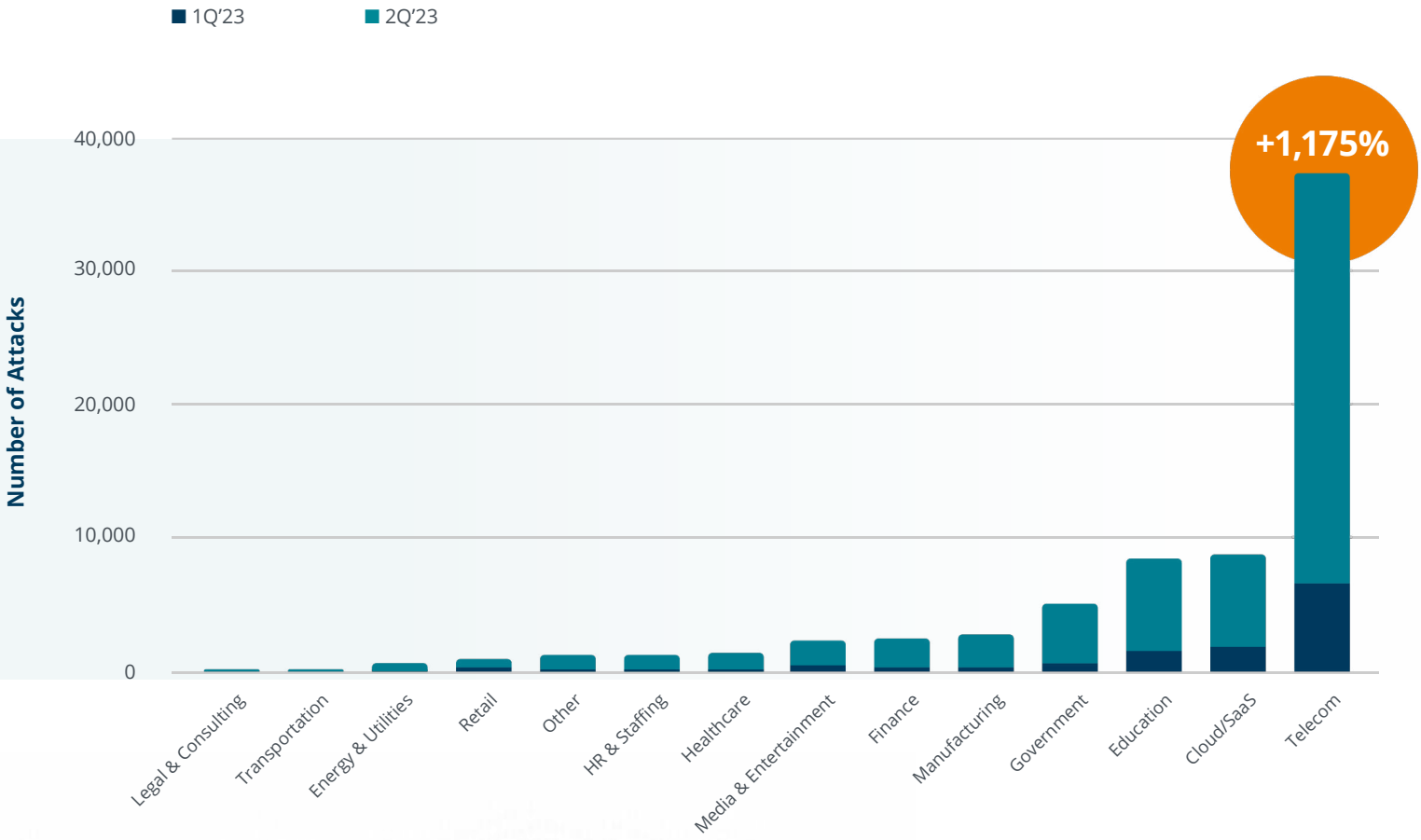
177% increase

The increase in DDoS attacks on government entities was likely driven by the rise in politically motivated cyber-attacks, such as those launched by Killnet. DDoS attacks here cause large-scale disruption and achieve high-profile publicity. Attackers can use DDoS to disrupt critical services, such as emergency response and elections.

Quarter Over Quarter

The massive growth of DDoS attack activity from 2022 to 2023 becomes even more striking when we witness the dramatic surge in attacks during the mere span of the last two quarters.

Total Number of Attacks Per Industry QoQ



Across industries, companies saw a **387% explosion** of attack activity from Q1 2023 to Q2 2023. **Why?**

- DDoS attackers are exploiting the ever-increasing sophistication of **AI and automation**
- Attacks are getting **easier to launch** for amateurs – they can simply, and cheaply, purchase a botnet attack
- Nation-state actors are sponsoring politically-motivated attack activity, such as Russian-affiliated attackers **Killnet, REvil, and Anonymous Sudan**

Let's Talk Telecom

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%**.

Why Telecom?

1. **Attacking the source:**
   Telecom providers are critical to communication and Internet services for all of us, making them a prime target for attackers seeking to cause chaos and disrupt services. They also have access to vast amounts of sensitive information, including financial data, which makes them an attractive target for cybercriminals.

2. **Large attack surface:**
   Telecom companies live online, and have a wide and diverse range of potential entry points that attackers attempt to exploit. These points include their digital assets, services, networks, equipment, and other infrastructure components. They're well protected, but if breached, are susceptible to being overwhelmed by DDoS attack traffic.

3. **Legacy technology:**
   The outdated systems of telecom providers are easier for hackers to exploit.

4. **Hacktivism:**
   DDoS attacks against telecom providers may have political motives, such as disrupting communication during a protest or silencing dissident voices.

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**.

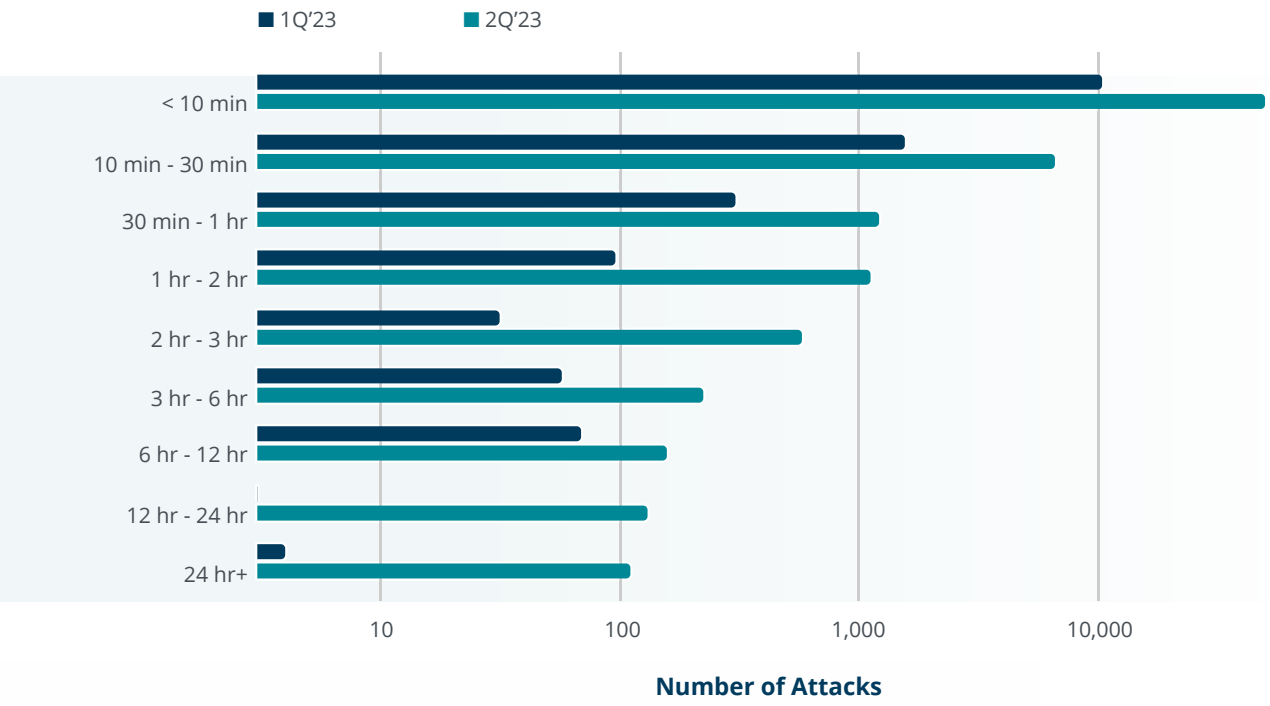
DDoS Protection is Everyone's Force Field

If your business is protected, the number of persistent 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.

The Duration of DDoS Attacks

Attacks are getting longer, **but over 83% of all attacks are still short-burst, lasting 10 minutes or less**.

Attack Duration Breakdown



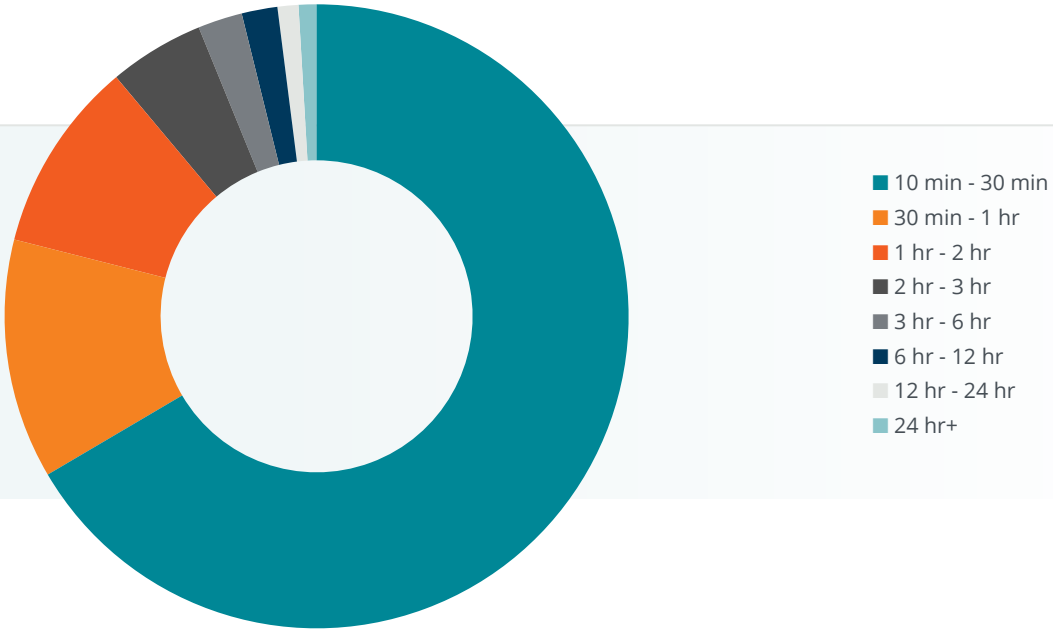
Why So Many Short Attacks?

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 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

Q1 and Q2, 2023



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:

Can customers interact with you if they can't connect using your network? Downtime hurts your reputation and hinders future business.

Employee experience:

Can your employees work remotely or in an office if they are not connected to your network? How long can you afford to be offline?

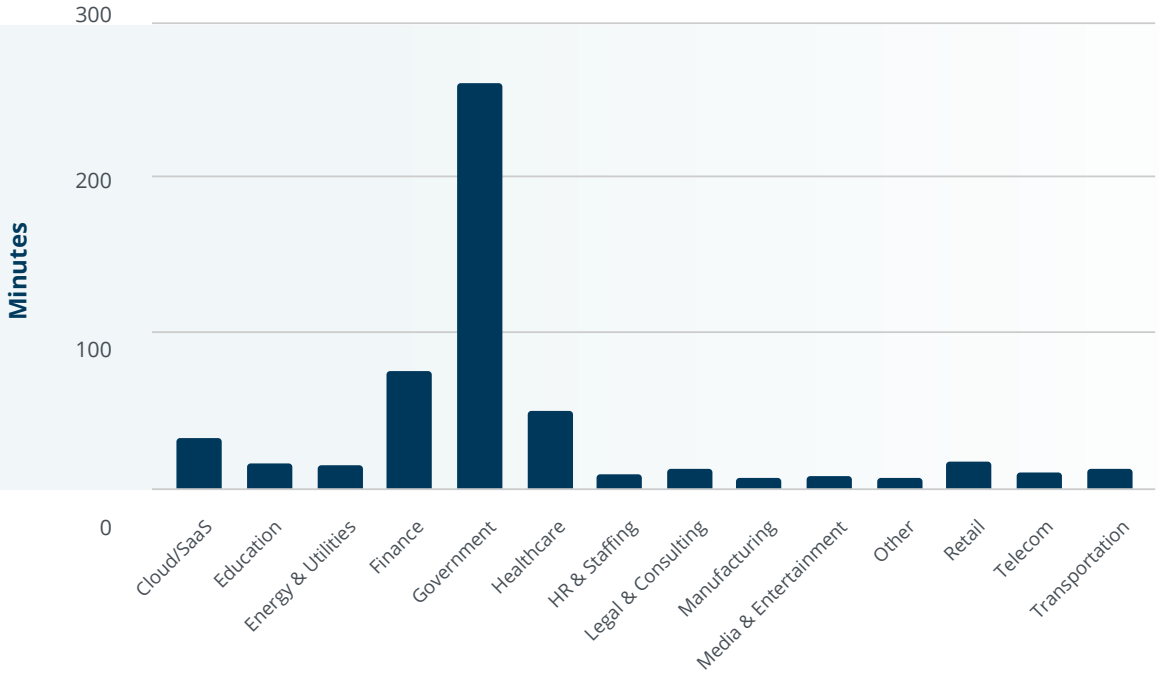
Financial impact:

What is the cost of fixing the network? Of regaining lost business? Of mending a damaged reputation?

The longest attack in Q1 was 10 days. The longest attack in Q2 was 42 days.
Even when attacks last for weeks, protected businesses are unimpacted.

Duration of Attacks by Industry

Q1 and Q2, 2023



Sustained Attacks Cause Special Harm

Government entities experienced the longest attacks with an average attack time of four hours and 20 minutes. Why?

1 **Political motivations:**

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.

2 **Complex infrastructure:**

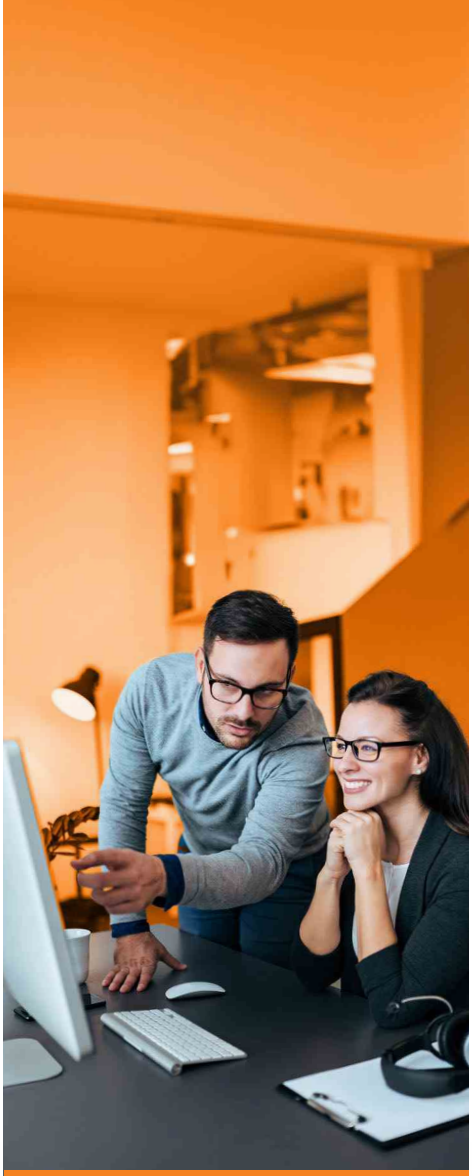
Government networks and systems are often complex and distributed, making them more challenging to defend against attacks. The larger the infrastructure, the more time it takes to detect and mitigate DDoS attacks, making them last longer.

3 **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.

Healthcare and **finance** providers experienced longer-than-average attacks as well. Both industries deal with a high value of sensitive information which can be used for 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.

Across all industries, the average **duration of attacks increased by 216%** in just one quarter.



From Q1 to Q2, the finance industry saw the biggest average attack duration increase: **from 41 minutes to 108 minutes.**

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.

No matter how long the attack, protected businesses are properly defended. The attack can last for hours, but with automated DDoS Protection, the attack has zero negative impact on your 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.

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

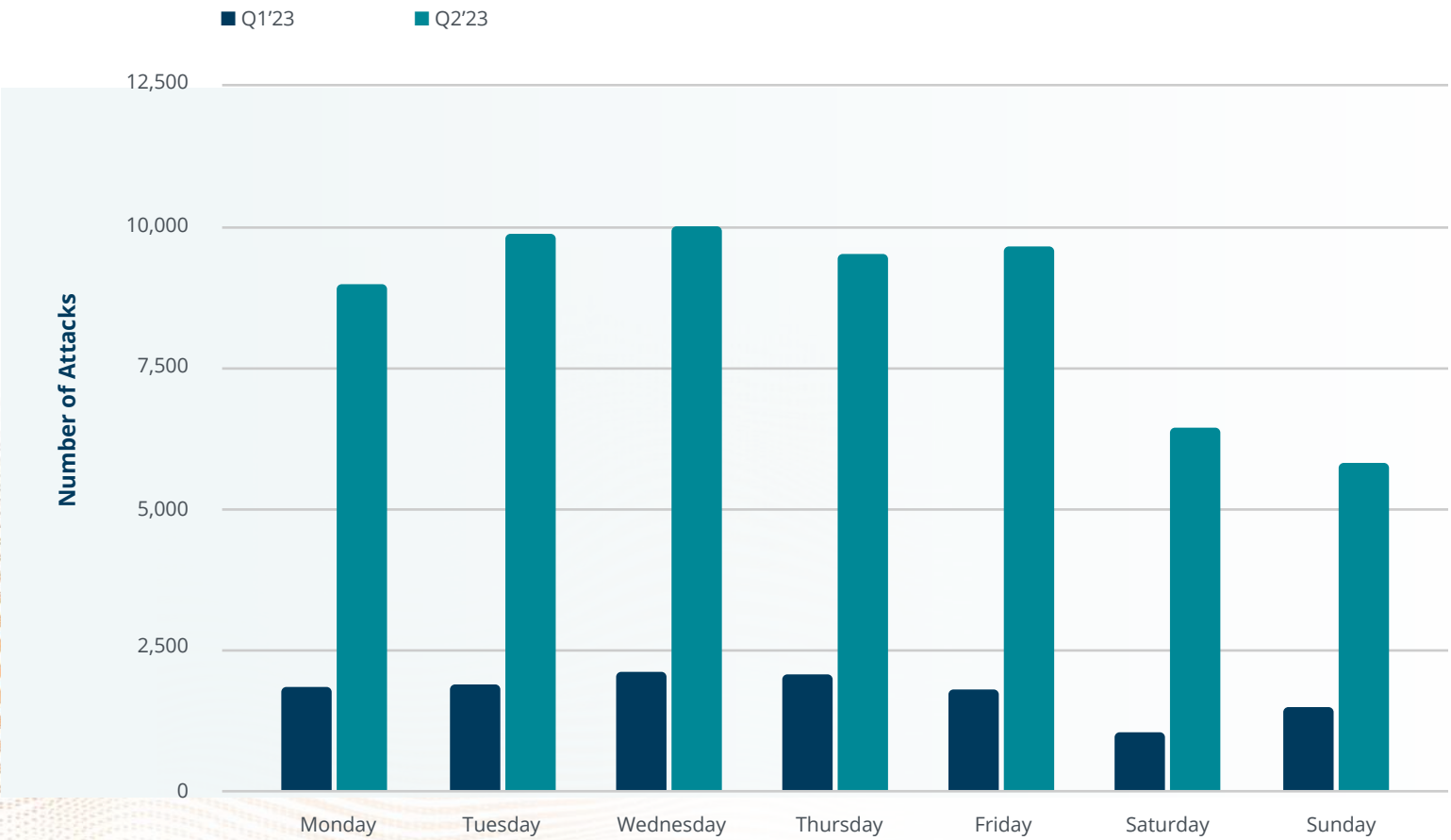
– **BILLY RUSSELL,**
Technology Director at North Judson-San Pierre Schools in North Judson, Indiana

The Time of DDoS Attacks

When will you be attacked? **When it hurts the most** – during the business week, during the business day. Even overseas hackers time their attacks to occur during the busiest period of your business day when your employees and customers need your network to work.

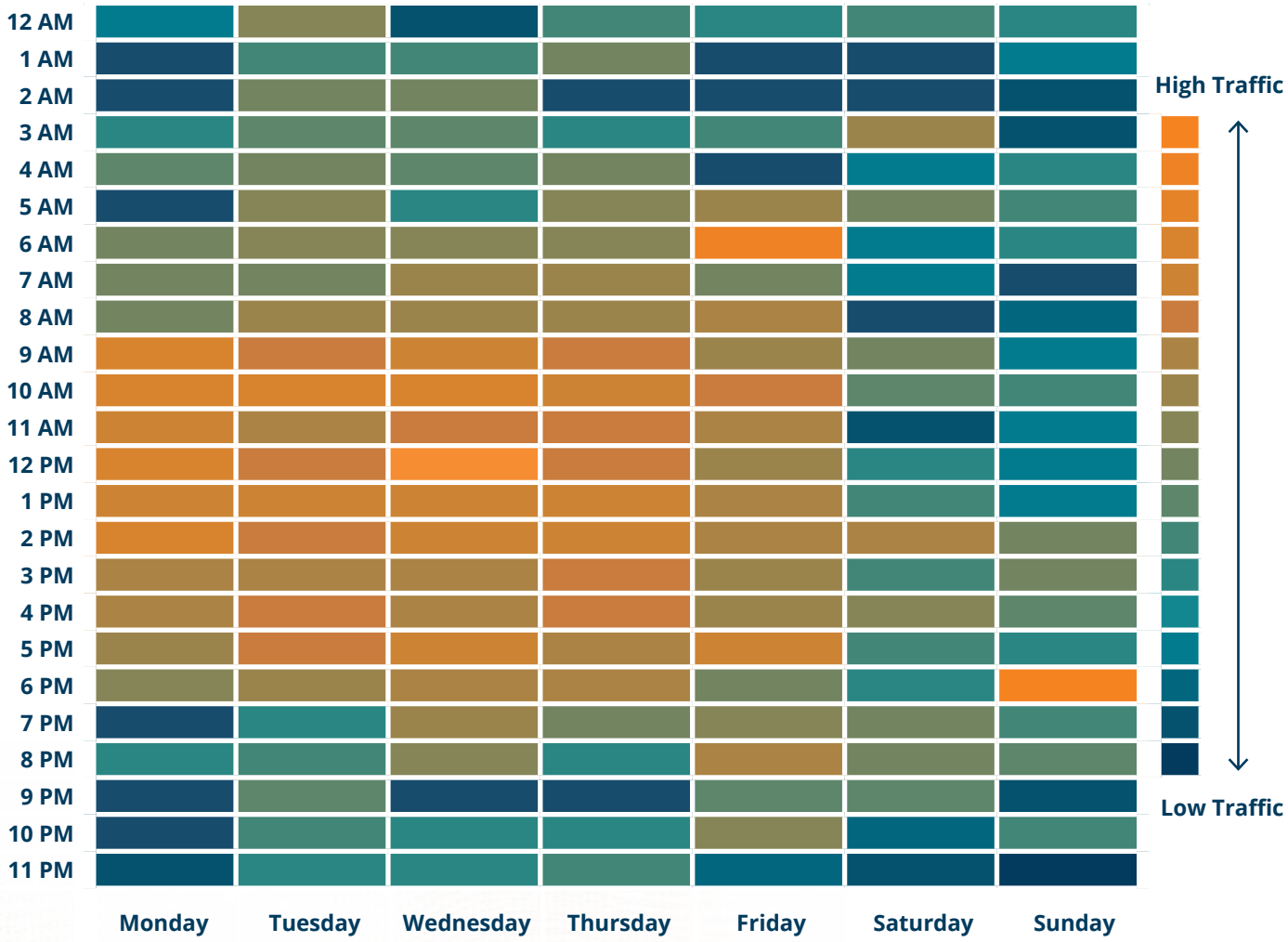
For every day of the week, Q2 saw a **4 fold increase** over Q1 in DDoS attack numbers.

When Attacks Occurred During the Week



When Attacks Occurred During the Day (Eastern Time)

Q1 and Q2, 2023



Findings and Conclusions:

Attacks occur most consistently during the Eastern U.S. business day. However, we're all online at all times, and large online consumer activity can result in outlier attacks outside of normal 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 in bandwidth can affect how long it takes to stop it and how damaging its effects are to your organization.

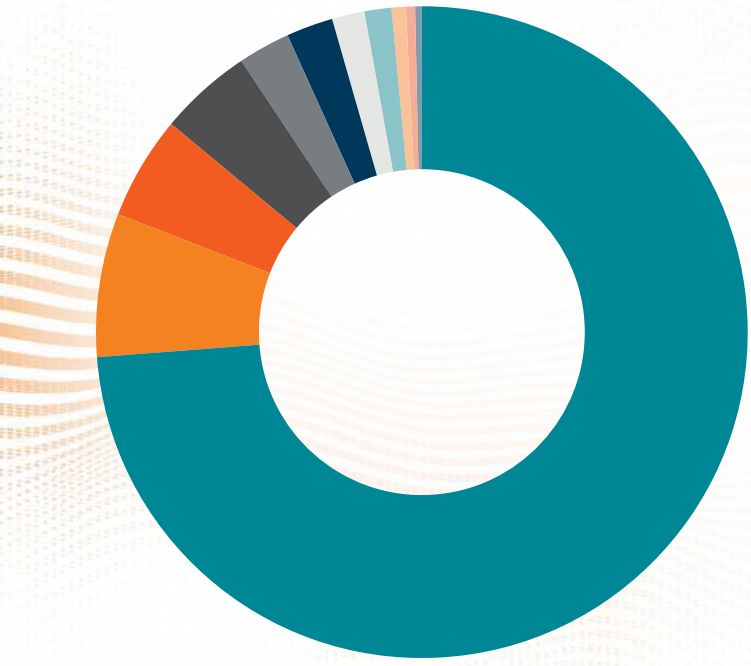
We saw that **media** and **retail** customers experienced the weightiest attacks on average, while the top 10% of attacks by size focused on **telecom**.

Average Attack Size per Industry

Q1 and Q2, 2023

Industry	Gbps
Media & Entertainment	3.5
Retail	3.1
Telecom	3.0
Energy & Utilities	2.4
HR & Staffing	2.4
Manufacturing	2.2
Healthcare	2.2
Cloud/SaaS	2.0
Government	1.9
Finance	1.3
Transportation	0.8
Education	0.7
Legal & Consulting	0.6
Other	0.5
Average	**1.9**

Of the Largest 10% of Attacks, Here's who was Targeted



Industry	1H'23
Telecom	73.71%
Media & Entertainment	7.12%
Government	5.13%
Cloud/SaaS	4.62%
Manufacturing	2.58%
Healthcare	2.32%
HR & Staffing	1.61%
Education	1.34%
Finance	0.70%
Retail	0.46%
Energy & Utilities	0.33%

Findings and Conclusions

The top five industries with the largest attack sizes are media, retail, telecommunications, energy, and staffing firms.

Why do 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.

The single largest attack Zayo saw during the first half of 2023 was a **980 Gbps** attack directed toward an on-line, publicly-networked **video communications company**. With more people working from home, this makes sense. A large attack aimed at the source of online video can impact the thousands of companies using that service.

1

Media and Entertainment

3.5 Gbps average attack size

Media and entertainment companies are attractive targets. They have a large online presence and access to sensitive data, such as valued intellectual property. Attackers use DDoS attacks to disrupt the distribution of content, damage reputations, and extort money. Successful attacks on this sector yield high publicity.

2

Retail

3.1 Gbps average attack size

From gaining a competitive advantage by eroding customer trust to extorting ransom, from ideological motives to disrupting peak shopping days, attackers have ample motivation to target retail's operations.

3

Telecommunications

3 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, with a significant overall impact.

4

Energy & Utilities

2.4 Gbps average attack size

The panic and distrust caused by disruption of critical infrastructure can lead to significant economic loss, making this segment a prime opportunity for attack profit through ransom. Whether financially or geopolitically motivated, large scale attacks to this industry can have much broader social or economic impacts.

5

HR & Staffing

2.4 Gbps average attack size

While seemingly less obvious, these firms are a key component of the supply chain of many other companies. Disruption here causes hiring disruptions across industries. Further, attackers may assume less cyber preparedness or increased software vulnerabilities in this industry - prime for an easy attack.

6

Healthcare, Manufacturing, and Cloud/SaaS

2.2 Gbps average attack size

These industries increasingly rely on digital technologies, AI, and IoT devices, increasing their attack surface and making them more vulnerable. Attackers see this tsunami of online traffic as a prime opportunity to fish for vulnerabilities.

Zayo's Stance

No Matter Your Company Size

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.

Protecting From the 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 robust DDoS Protection data, we decipher the underlying narrative within the data, presenting our informed conclusions for your consideration.

The first half of 2023 produced over **200 DDoS attacks per day**

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.

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

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.

Secure Your Business With Zayo Today

Learn more about protecting your business from a DDoS attack.

Contact us for immediate support.