REPORT

Lumen Quarterly DDoS Report

Q2 2022

LUMEN® TECHNOLOGIES

Executive Summary

The first half of 2022 has certainly been busy and full of surprises — two things you don't usually want to hear when you're reading about cybersecurity trends. The news reports about the ongoing slew of cyberattacks is enough to keep anyone awake at night.

That's why we have this report. The purpose of our Quarterly DDoS reports is to provide our readers not just an overview of what Lumen has observed but to put those attacks into context for you — answering the essential question: "Why should I care?"

Don't have time to read the full report? Here's what you need to know at a glance:

1 

There is an emerging trend of attackers leveraging **cloud-based virtual machine services** in a fraudulent way to significantly boost their attack capabilities.

2 

"Hit-and-run"-style attacks that are smaller in size and duration are being used to evaluate organizations' defenses.

3 

Bad actors are beginning to use **more surgical methods** when it comes to DDoS, instead of just relying on brute force.

Numbers you need to know:

1+ Tbps
was the largest bandwidth attack we scrubbed

72%
of attacks lasted less than 30 minutes

Telecomms, Software & Technology, and Gaming
industries were targeted by the largest attacks

LUMEN® TECHNOLOGIES

Table of Contents

LUMEN® TECHNOLOGIES

Key findings for Q2 2022

- The number of attacks mitigated decreased 26% compared to Q1 2022, and 14% annually.
- The largest bandwidth attack we scrubbed in Q2 was 1+ Tbps, which is the largest attack we've mitigated to date.
- The largest packet rate-based attack we scrubbed in Q2 was 246 Mpps, which is almost double what we mitigated in Q1.
- The longest DDoS attack period we mitigated for an individual customer lasted 21 days and 8 hours.
- 72% of attack period durations for our On-Demand DDoS customers were under 30 minutes in length.
- The most frequent day that attacks occurred were Tuesdays and Thursdays. The least frequent was Sunday.
- Multi-vector mitigations represented 38% of all DDoS mitigations, with the most common combination using DNS and TCP-SYN countermeasures.
- TCP-SYN flooding was the most common type of single-vector mitigation, accounting for 27% of DDoS mitigations.
- The top three targeted verticals in the 500 largest attacks were: Telecom, Software and Technology, and Gaming.

Inside a failed 1 Terabyte attack: A case study

Over the past few Quarterly DDoS Reports that Lumen has released, we have warned that attacks are getting larger and more complicated. The trend continued in the second quarter. In this section, we will be walking through a large-scale attack that we mitigated, sharing insights from Black Lotus Labs®, the Lumen threat intelligence team and providing you, the reader, with advice on how to protect your organization.

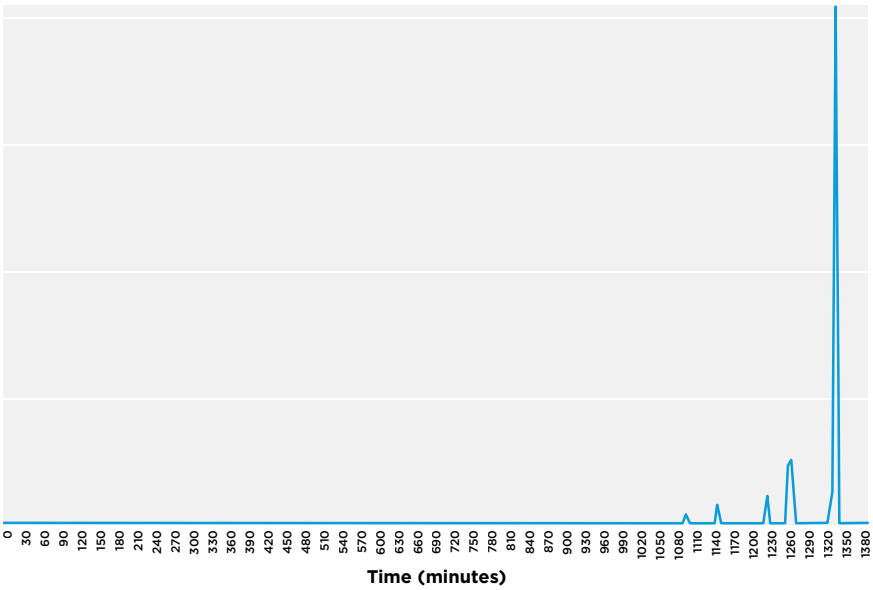
So what happened?

> "The large attack originated from 1,400 unique hosts, lasted about 12 minutes and resulted in a spike roughly 20,000 times larger than the target's normal traffic."

In Q2 2022, we prevented a 1+ Tbps attack from disrupting its intended target, a gaming service hosted by a telco that is a Lumen® DDoS Mitigation Service customer.[1] We observed three unique Command and Controls (C2s) issuing attack orders on four different dates and times against the victim. This activity all occurred within a week prior to the larger 1 Tbps attack, suggesting the attackers were testing attack methods and/or probing the target's network defenses.

The preceding attacks consisted of several different attack vectors, including TCP STOMP, where the threat actor attempts to bypass network countermeasures and/or overwhelm the host operating system, as well as application-specific attacks. The large attack, which was primarily UDP-based and originated from 1,400 unique hosts, lasted about 12 minutes and resulted in a spike roughly 20,000 times larger than the target's normal traffic
(see figure 1).

Figure 1. Traffic the day of the attack



LUMEN® TECHNOLOGIES

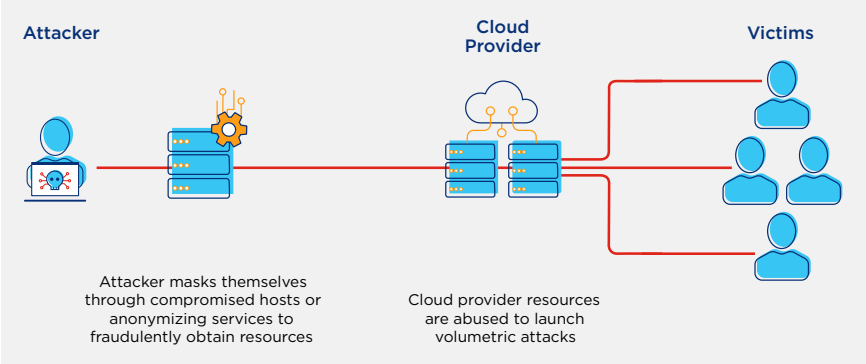
> “At the end of the day, neither the Lumen customer nor the intended victim experienced any disruption to their operations.”

At the end of the day, neither the Lumen customer nor the intended victim experienced any disruption to their operations. Without adequate protection, an attack much smaller than 1 Tbps could have taken both organizations offline for hours.

What’s different about this attack?

The size of this attack isn’t the only thing that’s notable. The attackers leveraged cloud-based virtual services in a fraudulent way to significantly boost their attack capability. There have been some notable virtual machine attacks recently and we expect this trend to continue. To be successful at this type of attack, cybercriminals mask their acquisition and control of cloud-based services through compromised hosts or anonymizing services. The cloud providers’ resources are then abused by the attacker to launch volumetric attacks against their intended victims (see figure 2).

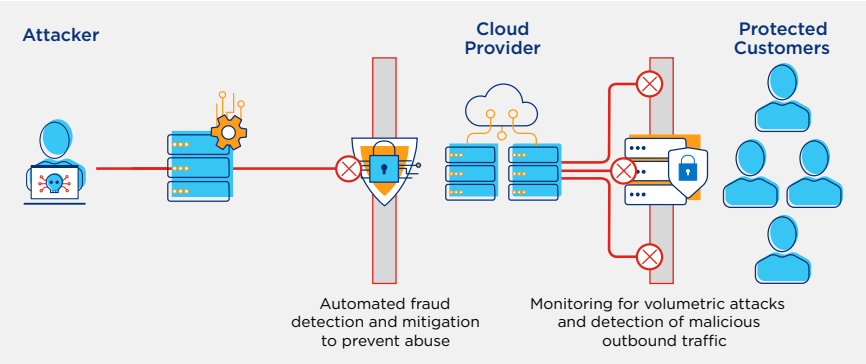
Figure 2. What a cloud services-based attack looks like



What should I be doing to protect myself?

This doesn’t sound great, so how do we stop it? The bulk of the work is on cloud providers. They should do their best to automatically detect and stop fraudulent accounts. Additionally, they should be monitoring activity coming out of their services to detect and stop malicious traffic from leaving their environments (see figure 3). While many have such mitigations in place, providers should remain vigilant as the tactics used by threats are ever-evolving.

Figure 3. How cloud service providers can help stop these attacks



LUMEN® TECHNOLOGIES

Here are some steps that you as an organization can take to avoid becoming a victim or having your cloud services abused to participate in attacks:

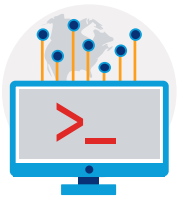
1 If you're using a cloud service, **ensure your accounts are protected by multi-factor authentication**. Account access and use should be routinely audited and follow good security practices.

2 **Keep your services that are hosted in the cloud up to date** (especially in terms of security patches) and monitor them for suspicious activity — like high usage rates.

3 If abuse is uncovered, **take appropriate mitigative actions** such as changing credentials, quarantining and cleaning impacted hosts, and removing or disabling any mechanisms that would allow the threat to persist within your cloud environment. In addition, consider alerting your cloud provider as the attack may have impacted multiple customers.

Misconception #1: Only the victims of attacks are affected?

Within research about DDoS attacks, there's a lot of focus on the victim of the attack – who was targeted, why they were targeted, and what they were targeted with. But DDoS attacks have a broader impact than just the victims. When an attack leverages a botnet (a network of infected devices), they are using legitimate devices, infecting them with malware and then using that botnet to launch attacks on other organizations. You don't want to be an unwitting participant in cyberattacks. Simply being part of a botnet can lead to increased bandwidth costs and performance issues for your online tools and applications. And once an adversary has access to your system, you're open to a myriad of attacks, from information stealing to crypto mining and ransomware.



Lumen mitigated

4,572

DDoS attacks in Q2.

▼26%

from Q1

50

attacks/day

How many DDoS attacks were there?

As with many trends, DDoS attacks experience seasonality, so there are going to be periods of time when attacks are more frequent. A new technique might come out and everyone rushes to try it or mimic it, while other times could see a lull in activity. In Q2 2022, Lumen mitigated a total of 4,572 attacks, a 26% decrease compared to Q1, which is traditionally a highly active period. On average, we were mitigating 50 attacks per day, with April 8 and April 13 experiencing the most attacks (111 and 108 respectively).

LUMEN® TECHNOLOGIES

How large are DDoS attacks?

There are two primary metrics for volumetric DDoS attacks:

Bandwidth attacks: Aim to disrupt service by flooding a circuit or application with traffic. This type of attack is measured in bits per second.

Packet rate attacks: Consume resources on network elements such as routers and other appliances, as well as servers. These are measured in packets per second with rates typically larger than bandwidth attacks.

Largest attack scrubbed

	Dropped bits/s	Dropped pkts/s
Q2 2022	1062 Gbps	246 Mpps
Q1 2022	775 Gbps	127 Mpps
QoQ change	▲37%	▲94%

Bandwidth attacks

We mitigated our largest bandwidth attack to date: more than 1 Tbps. This is a 37% quarter-over-over increase and 153% annual increase. To learn more about this attack you can go to Inside a Failed 1 Terabyte Attack earlier in this report.

The median attack size was 110 Kbps, which is a 43% decrease from last quarter. This could be from attackers using small attacks to probe organizations to see if they have DDoS mitigation.

Packet rate attacks

The largest packet rate attack nearly doubled from Q1, coming in at 246 Mpps. This is similar to the activity we saw in Q3 2021 – which was our most active quarter since we began releasing reports.

The median attack size was 123 Kpps which is a 35% decrease from the last quarter.

Misconception #2: It looks like the median attack size is reasonable to deal with. I don't need a mitigation service.

It's true, you're not likely to be hit with the largest attack on record. While DDoS attacks, in general, are becoming larger, our data shows attackers more frequently use small-scale attacks. We believe the bad actors are using these small-scale attacks as a probe to check on a victim's defenses. But keep in mind that every data point in this report has one thing in common — they were derived from customers that had DDoS mitigation. So, attackers could potentially see that our customers have protection and move along on their way to find someone else with a more vulnerable security posture.

Another reason to launch smaller attacks is because attackers can potentially distract an IT team with an abundance of small DDoS attacks while launching a more nefarious campaign elsewhere in the organization. No matter the cause – making sure your mitigation policy is current will help ensure that if a larger attack comes your way, there's no effect on your operations.

How long are attacks lasting?

Attack duration numbers are affected by the customer's mitigation model. There are two options.

1. On-Demand mitigation: Traffic is always monitored, but only scrubbed once a threat has been detected.
2. Always-On mitigation: Traffic is constantly being scrubbed to further minimize downtime.

The data points in this section only portray trends for On-Demand customers, which account for 73% of attacks mitigated in Q2 2022.

Do I need On-Demand or Always-On mitigation?

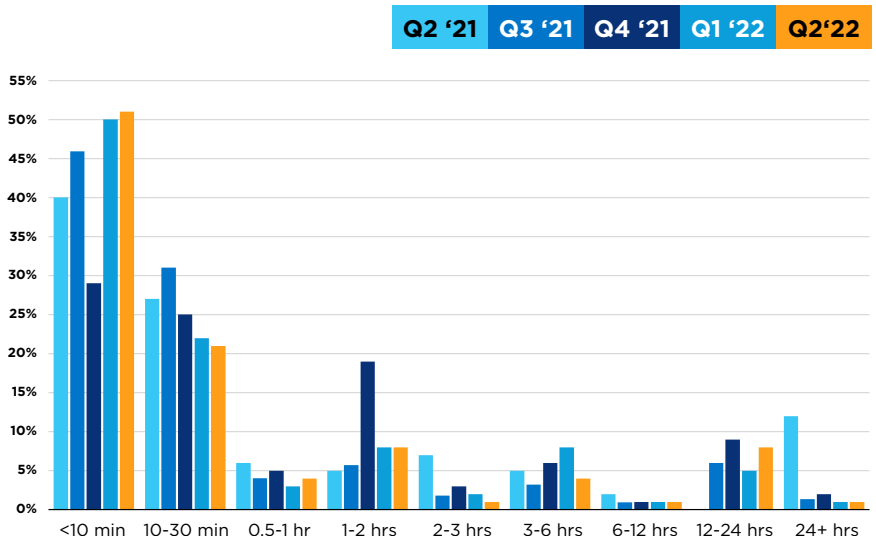
	Q2	QoQ change
Median attack duration	10m 0s	-
Average attack duration	3h 29m 40s	▲39%
Longest attack duration	21d 8h	▲336%

The longest attack period duration we mitigated was 21 days and 8 hours, which is the longest we have seen since we began issuing reports. This does not mean that there was a single attack that lasted 21 days; rather, there was an active campaign, which could have contained multiple attacks over time. This attack targeted one of Lumen's government customers, and the bad actor used a TCP-SYN attack method. Lumen was able to thwart the attack with TCP SYN Authentication countermeasures, but a large part was blocked by the customer's IP Location Policing which was set to block all traffic from specific countries.

The median attack size stayed on track with what Lumen saw in previous quarters. The average attack period duration increased by 39% quarterly, going from two and a half hours to three and a half hours. Both average and median attack-period durations saw an annual decrease of 20% and 33% respectively.

LUMEN® TECHNOLOGIES

Distribution by duration

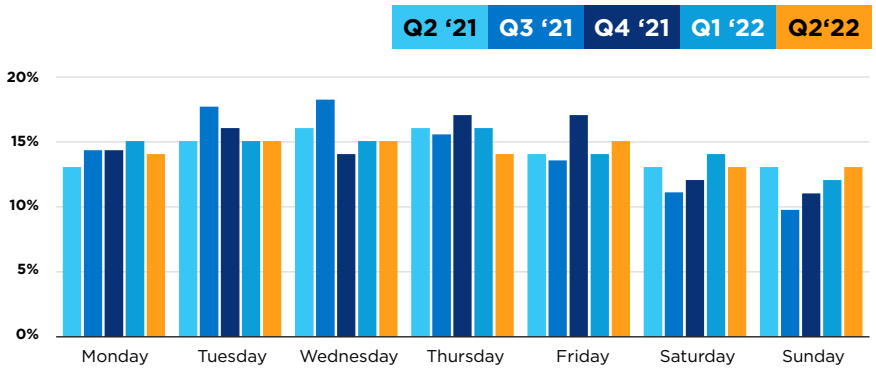


> "The longest attack period duration we mitigated was 21 days and 8 hours, which is the longest we have seen since we began issuing reports."

Half of all attacks on Lumen On-Demand mitigation customers lasted fewer than 10 minutes, which is in line with what we saw in Q1 2022. The second most popular attack-period duration was 10-30 minutes, representing 21% of activity. Similar to the trend we saw in attack sizes, the bad actors use quick hits to scope out defenses for potentially larger attacks, or they use this as a distraction for a bigger, nastier initiative.

We did see a jump in the 12–24-hour period. It represented 5% of activity in Q1 and jumped to 8% in Q2. This is notable because a year ago we didn't see any attacks fall in this range.

Distribution by day



Attacks continued to occur evenly throughout the week. Attackers were slightly more active on Tuesday and Thursday (16% each), while Sunday (as always) was the least active day at 12% of activity. This aligns with our observations that some cybercriminals operate like legitimate businesses, including having dedicated workweeks and holidays.

LUMEN® TECHNOLOGIES

Misconception #3: 10 minutes isn't that long to be down. I can get by with 10 minutes.

First, the 10 minutes of median attack duration is based on organizations that have active DDoS mitigation — if you don't have DDoS protection, attacks can be significantly longer. But let's put that aside for a minute — we would tend to agree with you that 10 minutes is not a long time in the grand scheme of things.

But think of everything you can do in 10 minutes: you can run a mile; you can cook a perfect medium-rare steak...**or** your customer could come to your site, see it's not working, and find what they're looking for with one of your competitors! How many customers interact with you every 10 minutes? Those are dollars walking right out the door simply because your website isn't available. Not only are you losing revenue, but now your customer support staff are dealing with angry customers and your IT team is scrambling to resume operations. DDoS attacks can have long-reaching and surprising ramifications for your bottom line, including fines or hits to your reputation.

What do DDoS attacks look like?

What is a multi-vector attack? Multi-vector attacks are layered DDoS attacks where cybercriminals use more than one method to attempt to disrupt an organization. Attackers do this for many reasons: part of the attack can handle different tasks, it's a way to increase the size of an attack, and they can target multiple entry points. These tend to be sophisticated and hard to mitigate without proper protection.

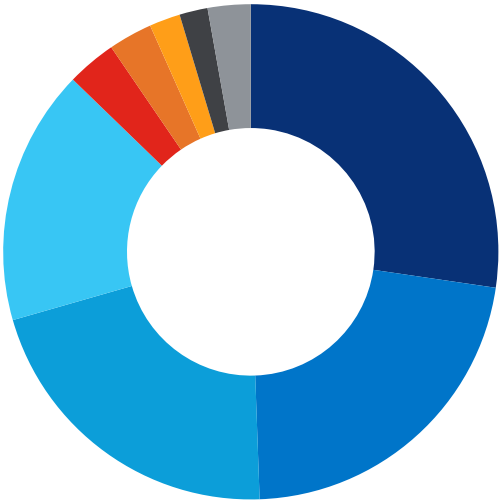
Multi/single-vector attacks

	Q1	Q2	QoQ change
Single-vector	62.2%	61.7%	▼.07%
Multi-vector	37.8%	38.3%	▲1.2%

Our single vs. multi-vector attack breakdown is the same as it was in Q1 2022, with a minimal increase in multi-vector attacks. While multi-vector attacks account for 38.3% of the total, they were much more prevalent in certain verticals such as telecommunications (70%), and gaming (58%).

Single-vector mitigations

Single-vector mitigation type breakdown



			QoQ
	TCP SYN	27%	↓15%
	UDP	22%	↑13%
	Static Filtering	21%	↑10%
	Invalid Packets	17%	↑4%
	DNS	3.22%	↓37%
	HTTP	2.87%	↑69%
	Other Volumetric	2.02%	↓37%
	SIP	1.84%	↑315%
	Other	2.80%	N.A.

When looking at the breakdown of single-vector mitigation types, TCP-SYN flooding continued to reign supreme for the second quarter in a row, accounting for 27% of activity. This was a 15% decrease compared to Q1 when TCP SYN accounted for 32% of mitigations; however, it is a 82% annual increase. This is a proven method for attackers to use because it does not require a large volume to disrupt the availability of service for targeted devices.

UDP-based amplification increased 13% quarterly and is on track with what we observed one year ago. UDP-based attacks aim to consume available bandwidth, and malicious actors like using this method because they can scale attacks with extraordinarily little effort. The initial attack can be amplified – doubling or even quadrupling – as the campaign progresses and becomes increasingly larger. If you're looking to learn more about UDP-based attacks, you can read our Q3 2021 Quarterly DDoS report, which includes a deep dive into the attack vector.

Static filtering continues to remain high among our single-vector mitigations at 21%, which is a 10% increase over Q1 but a 25% decrease compared to this time last year, when we saw this method leveraged heavily (28% of activity).

A vector we're going to be keeping our eye on is SIP (Session Initiation Protocol). SIP attacks impact VOIP infrastructure targeting vulnerable network resources and overwhelming them with high volumes of traffic. It tripled in activity compared to anything we've seen in previous reports, accounting for 1.84% of mitigations. While it is still low compared to tried-and-true methods, SIP is looked at as a more surgical attack method compared to brute force attacks like TCP-SYN flooding and UDP-based amplification.

Multi-vector mitigations

Top multi-vector mitigation type combinations

		QoQ
DNS, TCP SYN	20%	▲22%
TCP SYN, Static Filtering	7%	▼1%
Invalid Packets, UDP	4%	▲11%
UDP, Static Filtering	3%	▼33%
Invalid Packets, Static Filtering	3%	▲6%
Other Volumetric, UDP, Static Filtering	3%	▼4%
Other Volumetric, TCP SYN, UDP, Static Filtering	3%	▼37%
Invalid Packets, TCP SYN	2.34%	N.A.
Invalid Packets, UDP, Static Filtering	1.89%	N.A.
TCP SYN, UDP	1.77%	▼26%

For the second quarter in a row, DNS combined with TCP-SYN was the most popular type of multi-vector attack, accounting for 20% of activity in Q2. This is a 22% quarterly increase and over double what Lumen saw in Q2 of 2022. DNS Amplification is used because DNS is essential and cannot be turn off or blocked outright, additionally it provides a degree of anonymity to attacks. TCP-SYN is spoofed, providing an added level of anonymity, and can target service ports that cannot be blocked either. Both methods combined require more sophisticated than a "DENY" rule to defend against.

The second most popular combination was TCP-SYN combined with Static Filtering. This was used at the same rate as last quarter, but we saw a 64% increase over this period last year.

Other combinations we saw an increase in this quarter were Invalid Packets combined with TCP SYN (2.3% of mitigations), and Invalid packets combined with UDP and Static Filtering (1.89% of mitigations).

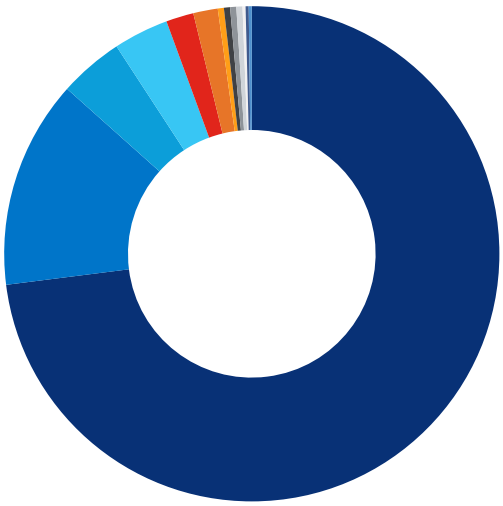
Misconception #4: As long as my network is protected, I'm all good.

While it's true that the network piece of your environment is the largest attack surface, digital advancements have led to a heavier reliance on applications for many businesses. Attackers have responded with much more layered, surgical and multi-faceted attacks. DDoS mitigation is most often focused on protecting against layer 3 and 4 attacks, but to get holistic protection for your environment, you need layer 7 protection as well. As we have observed this quarter with the increase in SIP attacks – attackers are pulling out new attack vectors in an attempt to get at your operations. Having bot management, API protection, and/or web application firewall can protect your digital assets so you don't have to react to an attack once it's already under way.

Learn about Lumen's award-winning application protection.

Who is getting DDoS attacked?

Largest 500 attacks by industry



Telecomm	73%
Software & Technology	14%
Gaming	4.2%
Government	3.6%
Hosting	1.8%
Finance	1.6%
Manufacturing	0.4%
Retail & Distribution	0.4%
Utilities	0.4%
Consulting	0.4%
Media & Entertainment	0.2%
Education	0.2%
Other	0.2%

Of the 500 largest attacks Lumen mitigated, 96% targeted these top five verticals (in order): Telecommunications, Software and Technology, Gaming, Government, and Hosting. It is important to note that when an attacker is targeting a telecommunications organization that doesn't mean that the telco is the intended target. The cybercriminal could be looking at targeting multiple victims within the telco's customer base.

Telecommunications

73%
of the largest 500 attacks

1,091
total attacks against vertical

Largest bandwidth attack:
1+ Tbps

Longest attack period duration:
6 days

70%
multi-vector attacks

Largest packet-based attack:
246 Mpps

Software and Technology

14%
of the largest 500 attacks

336
total attacks against vertical

Largest bandwidth attack:
90 Gbps

Longest attack period duration:
5 days

68%
single-vector attacks

Largest packet-based attack:
57 Mpps

LUMEN® TECHNOLOGIES

Gaming

4.2% of the largest 500 attacks

107 total attacks against vertical

Largest bandwidth attack: **20 Gbps**

Longest attack period duration: **4 days**

58% multi-vector attacks

Largest packet-based attack: **7 Mpps**

Government

3.6% of the largest 500 attacks

1,580 total attacks against vertical

Largest bandwidth attack: **39 Gbps**

Longest attack period duration: **21 days 8 hours**

63% single-vector attacks

Largest packet-based attack: **6 Mpps**

Hosting

1.8% of the largest 500 attacks

223 total attacks against vertical

Largest bandwidth attack: **6 Gbps**

Longest attack period duration: **2 days**

84% single-vector attacks

Largest packet-based attack: **2 Mpps**

Misconception #5: I don't see my industry in the graph above — I'm not a target.

If your industry is not on the list above, consider yourself lucky — you may not have experienced a major attack, but that doesn't mean you haven't been targeted. The chart above shows the 500 **largest** attacks, but we mitigated more than 4,000 attacks in Q2, and as we stated earlier in the report, attackers are using quick hit-and-run style attacks to disrupt operations, avoid detection, and test your defenses. Every organization nowadays is a target because every organization has some sort of data to protect. It could be employee data, customer data, or data about your technology — any form of data can be valuable to hackers, and DDoS attacks are commonly used as a distraction for a larger data breach or to extort payment. We have data on a variety of different verticals so if you're interested in seeing more about your industry, please contact a Lumen Sales representative to discuss.

Call us: 800-871-9244.

Final thoughts from Lumen

There are a lot of things that are outside of your control when it comes to cybersecurity. You have no influence over when, how, or if you're attacked. What you do have control over is how your organization chooses to respond to emerging threats. We've designed DDoS Hyper to make it deployable in minutes, to provide emergency mitigation during an attack.

Recommendations:

- At this point, DDoS mitigation is considered basic cybersecurity hygiene. Just like brushing your teeth to avoid cavities, having DDoS mitigation in place can deter attackers from launching large campaigns against your organization.
- Monitoring your network traffic can help detect if you're under attack, but it can also show if you're being used as a proxy in an attack against someone else. At that point it's a matter of finding, isolating and removing the malware.
- If your company uses applications to interact with customers, employees, or other stakeholders, having holistic protection against network AND application attacks will help ensure that your critical business functions stay up and running — even if you are under an active attack.
- While the perception is that it's easy to tell if you're under a DDoS attack, tactics are becoming more surgical and discreet. This. guide can help you find out if you're under an active DDoS attack.

Hopefully you have found this report to be interesting and engaging, and we want to thank you for your time and attention. If you would like to continue learning about the trends we have observed, you can read our past quarterly reports.

How can Lumen help me with DDoS mitigation?

With one of the largest DDoS mitigation deployments in the industry, backed by 170 Tbps of network-based mitigation capacity enacted at over 500+ multi-tiered scrubbing locations, Lumen owns DDoS mitigation at scale. You'll get to choose the mitigation level that is right for your organization with options like On-Demand or Always-On mitigation, and advanced features like intelligent scrubbing to help reduce latency and improve performance. You'll also be able to take advantage of a flat monthly service rate. You don't control the length, size or frequency of attacks so why should you be charged for it?

Visit our website to see what DDoS mitigation solution fits you best.

Need immediate protection? Lumen® DDoS Hyper® can be ready in minutes.

Learn more about our advanced DDoS Mitigation Service.

LUMEN® TECHNOLOGIES

1. This attack is reported under the telecommunications industry in our vertical breakdown because the Lumen customer of record was a telecommunications provider. You can see the full analysis in our vertical breakdown.

Methodology

Data in this report is from the timeframe of April 1, 2022 through June 30, 2022.

Scrubbed attacks are defined as either:

- Incidents flagged by high-level alerts mitigated by the platform, or
- Periods in running mitigations where individual countermeasures are dropping traffic, or
- Events where dropped traffic exceed passed traffic.

Attack vectors or mitigation types are identified either by countermeasures dropping traffic, or misuse types flagged in our flow-based monitoring.

Peaks in the data may be attenuated by how rates are averaged over various time increments.

Data from our Always-On customers is aggregated in increments of minutes, hours or days according to the length of time a mitigation runs. If a mitigation runs long enough that the resolutions time reaches a length of one day, and if there are multiple sequential days of attack, then it is counted as a single multi-day period of attack.

877-453-8353 | lumen.com | info@lumen.com

LUMEN® TECHNOLOGIES