REPORT

Lumen Quarterly DDoS Report

Q1 2022

LUMEN
TECHNOLOGIES

Introduction

We hope that you have had a great start to your 2022. The start of a new year is always exciting and brimming with possibilities: you have new budgets, new plans, new strategies, etc. The same can be true of bad actors. As cybercriminals operate more like legitimate organizations, they are going through the same things we all are, thinking about what ambitious projects they want to take on this year, where they are going to reinvest their revenue from 2021, and how they can expand their footprint. As you are thinking about what you need to accomplish this year, it is important to have the latest security trends at your fingertips to help determine areas of focus.

In our Lumen Quarterly DDoS report for Q1 2022 you will learn about:

- DDoS activity targeting Ukraine and what you can do to protect your organization
- Attack size, length and frequency
- DDoS attack vectors
- Targeted industries

For this report we examined data from the Lumen® DDoS Mitigation platform to develop our findings, which both reinforced and expanded on broader trends.

Table of Contents

Key Findings for Q1 2022 4

Will the Ukraine Conflict Affect Your Organization 5

DDoS Attacks by the Numbers 7

Attack Mitigation Types 12

Largest 500 Attacks by Industry 14

Key Takeaways 17

Key Findings for Q1 2022

- The number of attacks we mitigated increased 66% compared to Q4 2021 and 32% annually.
- The largest bandwidth attack we scrubbed in Q1 was 775 Gbps, which is the largest attack we've mitigated to date.
- The largest packet rate-based attack we scrubbed in Q1 was 127 Mpps, which was more than double what we mitigated in Q4.
- The longest DDoS attack period we mitigated for an individual customer lasted 5 days.
- 72% of attack period durations were under 30 minutes in length looking at our On-Demand DDoS customers.
- The most frequent day that attacks occurred was Wednesday.
- 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 mitigatation, accounting for 32% of DDoS mitigations.
- The top three targeted verticals in the 500 largest attacks were: Telecom, Gaming, and Software and Technology.

Will the Ukraine Conflict Affect Your Organization?

We couldn't put together this report without focusing on one of the biggest events going on in the world today: the Russian invasion of Ukraine. While this tragic event has had an enormous impact on the people of Ukraine, we are going to talk specifically about the cybersecurity implications of this continuing conflict.

In coordination with the physical attacks on Ukraine, we've seen ongoing cyberattacks ranging from wiper malware to continual and sustained DDoS attacks of Ukrainian and critical infrastructure from neighboring countries. Ukraine's State Service of Special Communications and Information Protection said that "Russian hackers keep on attacking Ukrainian information resources nonstop." These DDoS attacks have not gone without response — according to Wired, Russia is being hit with similar attacks from hacktivist groups and, in some cases, Ukrainian-enlisted hackers.

With so many developments, the threat intelligence arm of Lumen, Black Lotus Labs®, is monitoring Russian threat activity both in the region and around the world. Black Lotus Labs is working with industry partners, including the Joint Cyber Defense Collaborative (JCDC), as we continue to monitor the evolving situation in Ukraine, whether through analyzing DDoS traffic visible on the Lumen backbone or identifying C2 infrastructure being used to wage attacks. Learn more about Lumen's readiness to meet global events.

Although DDoS activity is currently limited to the region, that doesn't mean that it will continue to stay that way. If you're worried about protecting your organization, Lumen suggests following the advice provided by the Cybersecurity & Infrastructure Security Agency (CISA):

1. Reduce the likelihood of a damaging cyber intrusion

a. Validate that all remote access to your organization's network and privileged or administrative access requires multi-factor authentication.

b. Ensure that software is up to date.

c. Confirm that your organization's IT personnel have disabled all ports and protocols that are not essential.

d. If your organization uses cloud services, ensure they have been reviewed and implement strong controls.

2. Take steps to quickly detect a potential intrusion

a. Ensure your staff are focused on identifying and quickly assessing any unexpected or unusual network behavior.

b. Confirm that your organization's entire network is protected by up-to-date antivirus/anti-malware software.

c. If you do work with Ukrainian or Russian organizations, take extra care to monitor, inspect and isolate traffic from those organizations.

3. Ensure your organization is prepared to respond if an attack occurs

a. Designate a crisis-response team along with roles and responsibilities across technology, communications, legal and business continuity departments.

b. Conduct a tabletop exercise to ensure that everyone knows their roles during an active incident.

4. Maximize your organization's resilience to a destructive cyber incident

a. Test your backup procedures to ensure that your critical data can be quickly restored.

b. If you use industrial control systems or operational technology conduct a test of manual controls so critical functions remain operable.

Everything listed above can seem incredibly overwhelming. But it doesn't have to be. Lumen can assist with finding vulnerabilities within your organization, evaluating your security frameworks and providing your team recommendations to achieve your desired security posture.

Learn more

What is Black Lotus Labs?

Black Lotus Labs is the threat intelligence team within Lumen. It is a group of security professionals and data scientists whose mission is to leverage Lumen's global network visibility to both help protect your business and keep the internet clean. Black Lotus Labs uses threat hunting and analysis, as well as machine learning and automated threat validation, to identify and disrupt the work of malicious actors. If you're interested in learning more about the latest research and advanced actor and crimeware tracking capabilities of Black Lotus Labs, read their blogs.

Read now

DDoS Attacks by the Numbers

After a relatively quiet fourth quarter, 2022 is starting off with a bang. Lumen mitigated 6,162 DDoS attacks in the first quarter, which is a 66% increase from Q4 and a 32% increase from what we saw in Q1 2021. On average Lumen mitigated 70 attacks daily, which is a 63% quarter-over-quarter increase. The days with the most attacks were March 30 (150 attacks), January 24 (139 attacks), and tied for third were March 17 and March 27 (125 attacks).

Attack Size and Duration

Largest Attack Scrubbed

	Dropped Bits/s	Dropped Pkts/s
Q1 2022	775 Gbps	127 Mpps
Q4 2021	499 Gbps	60 Mpps
QoQ Change	▲55%	▲112%

There are two primary metrics for volumetric DDoS attacks:

1. **Bandwidth Attacks:** These aim to disrupt service by flooding a circuit or application with traffic. This type of attack is measured in bits per second.
2. **Packet Rate Attacks:** These 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.

Bandwidth Attacks

We mitigated our largest bandwidth attack since we started our report: 775 Gbps. This is a 55% quarterly increase and a 189% annual increase.

The average attack size mitigated was 2 Gbps, which is what we have observed in previous Lumen reports.

Packet Rate Attacks

The largest packet rate attack more than doubled compared to Q4, going from 60 Mpps to 127 Mpps.

There is a monumental jump in the largest attack size when looking at annual comparisons: in Q1 2021 the largest attack was 26 Mpps, showing an annual increase of more than 380%.

The average attack size was 477 Kpps, which is a slight decrease compared to Q4 2021, but still higher than the rest of the data presented in 2021.

Takeaway #1

Why should I care about attack sizes?

With attack sizes continuing their trend of increasing in size, it's obvious that cybercriminals are escalating to match new defensive measures and overwhelm targets with larger-than-life botnet infrastructures. While it's true you might not be hit with the largest DDoS attack in history, there's a good chance you're going to be hit by a DDoS attack, if you haven't already. Organizations without DDoS mitigation services in place can easily be taken offline by a 1 Gbps attack. Having a DDoS mitigation solution will not prevent you from being attacked; however, it will help ensure that your organization can continue with normal operations during an active attack.

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 below only portray trends for On-Demand customers, which account for 69% of the attacks Lumen mitigated in Q4. Learn more about the differences between On-Demand and Always-On mitigation.

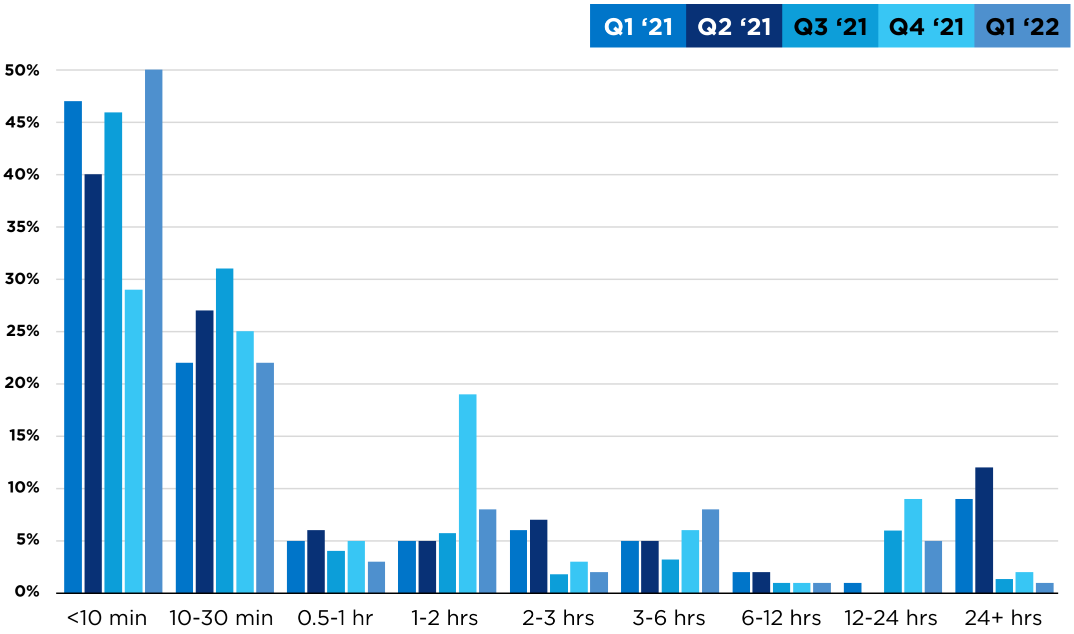
Watch Video

	Q1	QoQ Change
Median attack duration	10m 0s	↓67%
Average attack duration	2h 37m 55s	↓44%
Longest attack duration	5 days	0%

There were decreases in both median and average attack period durations compared to Q4 2021; however, during that quarter, we had experienced longer attacks than in previous quarters. The data for Q1 is on par with what was mitigated during the rest of 2021. The median attack period duration was 10 minutes, which is a 67% quarterly decrease from Q4 (30-minute median attack duration), and an annual decrease of 33% compared to Q1 2021 (15-minute median attack duration).

The longest attack period duration period was five days, which remained steady quarter over quarter. It is a decrease from what we saw in Q1-3 of 2021, which saw the longest attack periods over 10 days. This doesn't mean we can all relax; cybercriminals are not giving up. Like any business, cybercriminal organizations aim to realize efficiencies and they are running larger, more effective attacks more quickly. As 2022 progresses, we can expect to see this data fluctuate based on attackers' new tactics. It's important to note that attack period duration doesn't just indicate the length of a single attack — an organization can experience a flurry of attacks during a duration period.

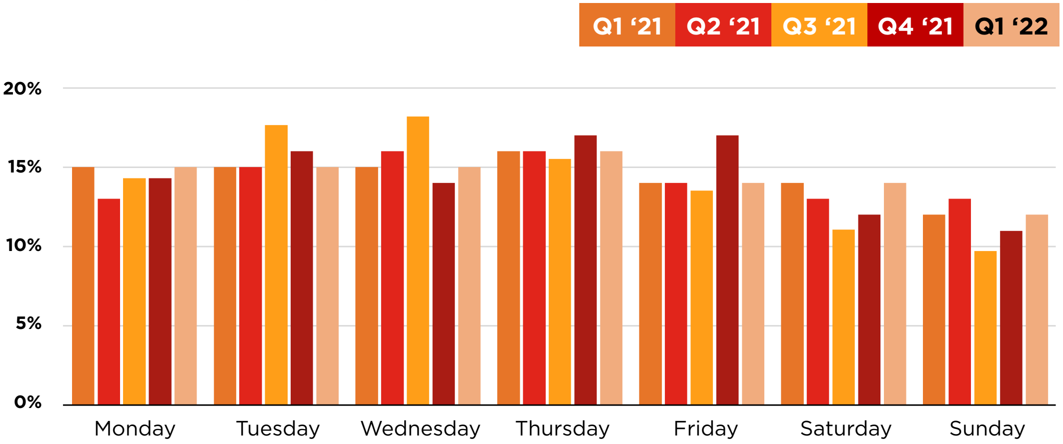
Distribution by Duration



Half of all attacks on Lumen On-Demand mitigation customers lasted less than 10 minutes, which is the highest percentage of activity that we've seen compared to previous reports. This could mean those bad actors are focused on quick hits, and they're probing attacks to test an organization's defenses before implementing larger-scale attacks.

The second most popular attack period duration was 10-30 minutes, representing 22% of activity. There was also a slight uptick in attacks lasting three to six hours, going from 6% of activity in Q4 to 8% of activity in Q1 2022. We've observed a decline in the reliance on longer attack period durations. Attacks over 24 hours have experienced an 85% annual decrease.

Distribution by Day

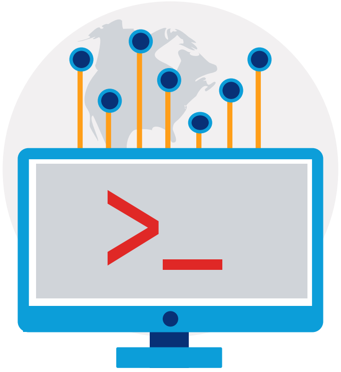


Attacks occurred evenly throughout the week; however, they were slightly more likely to occur Monday through Thursday (~15% of attacks per day) vs Friday through Sunday (~13% per day). This aligns with our observation that cybercriminals operate similar to businesses including having dedicated workweeks.

Takeaway #2

Why should I care how long attacks last?

If you're a digital organization today, then you're extremely reliant on your website, applications, tools, and your computing power overall. Can any of those things experience any downtime? Will your employees function? Can your customers interact with you? The cost of an attack isn't just that your web-facing assets won't work, but the downtime you suffer can have long-reaching ramifications for your bottom line including fines or hits to your reputation. In recent years, the average cost of a DDoS attack can be in the hundreds of thousands of dollars.



Attack Mitigation Types

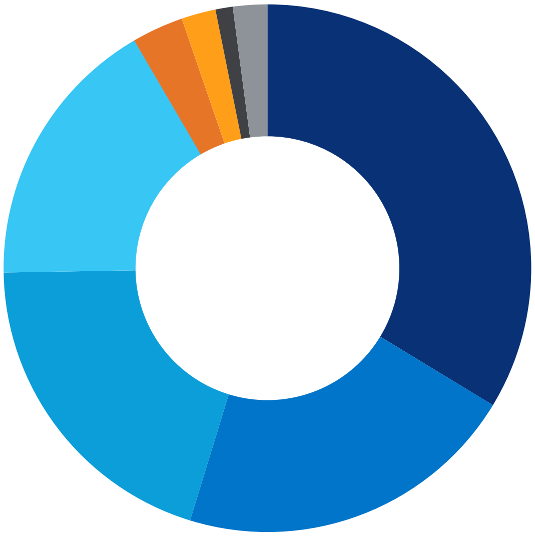
Multi/Single-Vector Attacks

	Q1 2022	Q4 2021	QoQ Change
Single-vector	62%	65%	▼4%
Multi-vector	38%	35%	▲8%

In Q1, single-vector attacks continue to be the primary method used by bad actors, even with a 4% quarterly decrease. Findings continue to be on par with previous reports' data. Multi-vector attacks represented 38% of total attacks, but much higher in verticals such as gaming (80%) and telecommunications (67%).

Single-Vector Mitigations

Single-Vector Mitigation Type Breakdown



			QoQ
■	**TCP SYN**	32%	▲148%
■	**UDP**	20%	▼33%
■	**Static Filtering**	19%	▼19%
■	**Invalid Packets**	16%	▼37%
■	**DNS**	0%	▲412%
■	**Other Volumetric**	3%	▲7%
■	**HTTP**	2%	▲70%
■	**IP Fragmentation**	1%	▼6%
■	**Other**	2%	▼29%

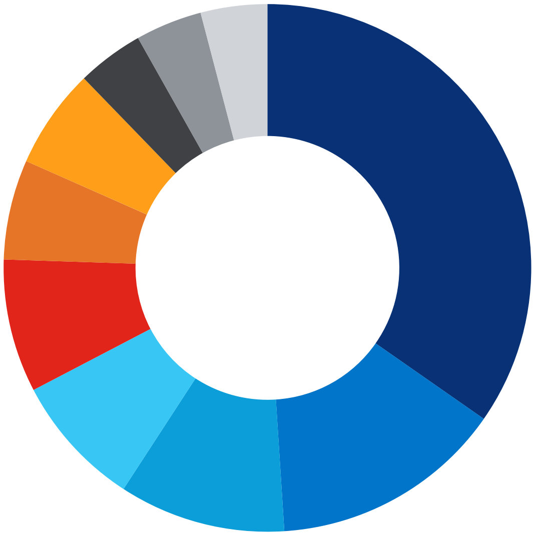
When looking at the breakdown of single-vector mitigation types, TCP-SYN jumped right to the top of the list going from 13% of activity in Q4 2021 to 32% of activity in Q1 2022, which is a 148% increase quarterly and 61% increase annually. This could mean that attackers are relying on simpler, tried-and-true attack methods for the most optimal results.

UDP-based amplification mitigations went from the number one spot down to the second spot. This was a 33% decrease compared to Q4, but in line with what we found throughout the rest of 2021. UDP-based attacks aim to consume available bandwidth and have proven to be quite powerful with the ability to generate attacks many multiples of the size of the initial bytes sent. If you're looking to learn more about UDP-based attacks you can read our Q3 2021 Quarterly DDoS report, which does a deep dive into the attack vector.

Static filtering continues to remain high among our single-vector mitigations at 19%, which was a 19% decrease compared to Q4, but still on par with the rest of our findings from 2021. Static filtering countermeasures are typically done on items such as port and protocol. These statistics also include known bots and abused reflectors as discovered by Black Lotus Labs, which provides initial mitigation against attacks.

Multi-Vector Mitigations

Top Multi-Vector Mitigation Type Combinations



			QoQ
■	**DNS, TCP SYN**	17%	▲38%
■	**TCP SYN, Static Filtering**	7%	▲65%
■	**UDP, Static Filtering**	5%	▼3%
■	**Other Volumetric, TCP SYN, UDP, Static Filtering**	4%	N.A.
■	**Invalid Packets, UDP**	4%	▼41%
■	**Other Volumetric, UDP, Static Filtering**	3%	▼35%
■	**Invalid Packets, Static Filtering**	3%	▼16%
■	**TCP SYN, UDP**	2%	▲20%
■	**Other Volumetric, TCP SYN, UDP**	2%	N.A.
■	**Other Volumetric, UDP**	2%	▼49%

The multi-vector mitigations represented 38% of activity, with the most common using a DNS query flood combined with a TCP SYN flood (17% of multi-vector mitigations). Lumen observed a 38% quarterly increase in this combination and a 28% annual increase. This was the most leveraged attack method throughout most of 2021, specifically in Q4, Q2, and Q1. DNS-based DDoS attacks here refer to DNS floods, where attackers seek to disrupt Domain Name System servers to prevent DNS resolution of a given domain. These attacks often randomize questions so that DNS' natural caching mechanisms will not protect the server.

Other combinations include TCP SYN and Static Filtering (7% of activity) and UDP-based amplification and Static Filtering (5% of activity).

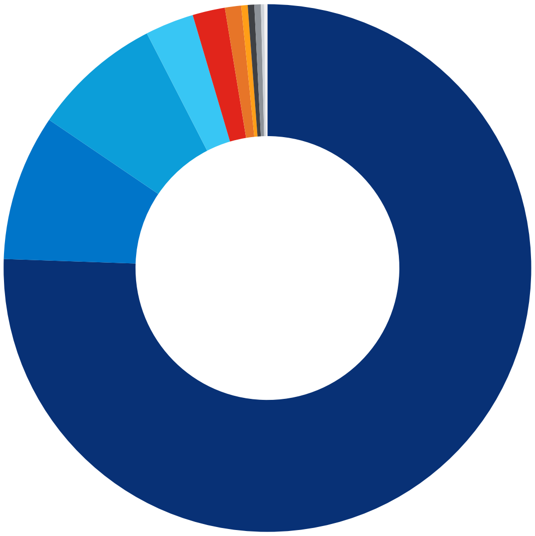
Takeaway #3

Why should I care about what attack vectors are being used?

Cybercriminals are constantly changing their attack vectors in response to new defense strategies their encounter. Bad actors are motivated to continue modifying their attacks until they break through. It's an ongoing escalation race between attackers and defenders. This can lead to overburdened security teams who are trying to keep up with the latest tactics. The Lumen Black Lotus Labs threat intelligence team works every day to defend our global community from malicious activity. Their threat intelligence is fed into our DDoS mitigation solutions and other managed security solutions through our Rapid Threat Defense capability.

Read data sheet

Largest 500 Attacks by Industry



Telecomm	76%
Gaming	9%
Software & Technology	8%
Hosting	3%
Government	2%
Education	1%
Other	0.4%
Finance	0.4%
Business Services	0.4%
Banking	0.2%
Media & Entertainment	0.2%

Of the 500 largest attacks, 97% targeted these top five verticals (in order): Telecommunications, Gaming, Software and Technology, Hosting, and Government.

It is important to note that a single customer contributed to most of the telecommunication attacks we mitigated. Over the first quarter, they were attacked more than 1,300 times. This doesn't mean that the target was specifically the telecommunications company, as there could be multiple targets within their customer base. Below you can find more details on our top targeted industries.

Telecommunications

76% of the largest 500 attacks	1,487 total attacks against vertical	Largest bandwidth attack: 775 Gbps
Longest attack period duration: 4 days	67% multi-vector attacks	Largest packet-based attack: 70 Mpps

Gaming

9% of the largest 500 attacks	167 total attacks against vertical	Largest bandwidth attack: 93 Gbps
Longest attack period duration: 4 days	80% multi-vector attacks	Largest packet-based attack: 17 Mpps

Software and Technology

8% of the largest 500 attacks	419 total attacks against vertical	Largest bandwidth attack: 18 Gbps
Longest attack period duration: 4 days	68% single-vector attacks	Largest packet-based attack: 3 Mpps

Hosting

3% of the largest 500 attacks	108 total attacks against vertical	Largest bandwidth attack: 111 Gbps
Longest attack period duration: 5 days	76% single-vector attacks	Largest packet-based attack: 11 Mpps

Government

2% of the largest 500 attacks	2,447 total attacks against vertical	Largest bandwidth attack: 110 Gbps
Longest attack period duration: 2 days	66% single-vector attacks	Largest packet-based attack: 11 Mpps

Takeaway #4

Should I care about DDoS attacks if I don't see my vertical on the list above?

The short answer is yes. The sectors listed above were targeted this quarter; however, nearly every vertical and every type of organization can and is attacked regularly. A question to ask yourself is: do I have any sort of data that someone might want to attack? Desirable data includes customer information, employee information, or privileged knowledge. If you want to learn more about attack trends in your vertical, please contact a Lumen sales representative to discuss.

Contact us

Key Takeaways

The biggest thing we hope you take away from reading our Quarterly DDoS Reports is that security should not be an afterthought; rather, it needs to be a conscious effort by every part of an organization. With nation-states playing a bigger role in the attack landscape, there are going to be bystanders that get attacked even if you aren't the intended target.

As you are thinking about your own security posture, ask yourself: what would you do if your organization was attacked tomorrow. Our data shows that DDoS attacks, while they ebb and flow, are getting larger, more pervasive, more complex, more widespread and lasting longer.

Wondering if you're under a DDoS attack?

Learn to recognize the signs: How to Tell if Your Business is Suffering from a DDoS Attack.

What do I do if I currently have no DDoS protection?

If you don't have a DDoS mitigation partner or you're looking for a new one, here are some questions to ask potential providers:

- How do you handle large attacks?
- If one of your other customers is attacked, how will it affect my organization?
- What does your scrubbing architecture look like? Is it global?
- Do you do anything to block threats before they become attacks?
- From where do you receive your threat intelligence to block new threats? Is that threat intelligence integrated into your solutions?
- Do you have employees working in a variety of locations, and can you support hybrid work models?

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 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 size, length or frequency of attacks so why should you be charged for it?

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

Learn more about Lumen DDoS Mitigation Service

Learn more about Lumen® DDoS Hyper®

If you're interested, read our 2021 quarterly reports

Methodology

Data in this report is from the timeframe of January 1, 2022, through March 31, 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 resolution 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

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice. ©2022 Lumen Technologies. All Rights Reserved.