REPORT

Lumen Quarterly DDoS Report

Q4 2022

LUMEN®

The Platform for Amazing Things℠

Executive Summary

Another year has ended which means it's time to reflect on the lessons learned in 2022 that we can take with us to protect our organizations, our employees and our customers in 2023.

The purpose of the Lumen Quarterly DDoS Reports is to provide you with an overview of the DDoS attacks we mitigated and put them into context for you. We seek to help you answer the essential question: "Why should I care?" and "what can I do about this?"

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

1 **Attackers are trying to fly under the radar:** Threat actors are using essential services and expected forms of traffic such as DNS to fly through defenses.

2 **Holidays are ideal for adversaries:** Attackers are looking to take advantage of understaffed IT and security teams.

3 **"Hit-and-run"-style attacks are evolving:** Small, quick attacks are still being leveraged, but we're seeing the same victims targeted multiple times to cause long-term chaos.

Numbers you need to know for Q4 2022:

DDoS attacks increased **66% quarter over quarter.**

Quick hit attacks (under 30 minutes) accounted for **89% of attacks.**

The largest attacks targeted the **Telecoms, Software & Technology, and Gaming** industries.

Table of Contents

2022 by the numbers

Total attacks mitigated:

25,476

↑ 22% from 2021

Largest bandwidth attack:

1.06 Tbps

↑ 73% from the largest 2021 attack

Largest packet rate attack:

246 Mpps

↓ 2% from the largest 2021 attack

Average bandwidth attack size:

1.5 Gbps

Average packet rate attack size:

426 Kpps

Average attack duration:

2.5 hours

Most common single-vector attack methods:

Domain Name System (DNS) Amplification

and

TCP-SYN Flooding

Percentage of attacks that were multi-vector:

39%

Most targeted industries:

Telecoms

Government

Software & Technology

What DDoS trends will 2023 bring?

Reflecting on the past year, let's be honest: we survived some things! We saw some workforces return to offices en masse, while other organizations adopted hybrid work models. Throughout the year we've seen massive layoffs after a few years of massive growth. And 2022 started off with what can be the new face of warfare — cyberwar activities between Russia and Ukraine.

As we think about the possibilities ahead in 2023, one thing is certain: cyber attackers will continue to keep us on our toes. In this section, we will summarize our observations from the past 12 months, and consider which opportunities attackers might attempt to exploit in 2023.

2022 trends

The changing landscape of warfare

The conflict between Russia and Ukraine came to a head in February 2022. The world watched as this David versus Goliath epic unfolded, and while this conflict has played out in the "real world" with a real human toll, this war is one of the first to have significant levels of cyber operations on both sides.

Russia came in with brute force attacks to overwhelm infrastructure and also leveraged cyber intelligence to determine areas of focus. However, Ukraine has held its own. After defending against Russian cyberattacks for nearly a decade and with support from other countr ies, they learned a thing or two and were able to implement defenses that could outpace Russian attacks.

We also saw these cyberattacks bleed into the private sector, with many organizations pulling operations out of Russia. If you're interested in reading more you can read our Q1 2022 report or this great article from Carnegie Endowment for International Peace.

Attackers are leaning into hit-and-run attacks

Throughout all of 2022 Lumen was mitigating a large quantity of attacks that were small in both size and duration (less than 10 minutes and under 5 Mbps). And the big question was "why"? There are a few reasons threat actors leverage small-scale attacks.

Where does this threat intelligence come from?

This report is developed with the participation of a few teams — our DDoS mitigation operations team and our Black Lotus Labs® team work together to come up with insights for our readers.

BLACK LOTUS LABS®

Black Lotus Labs is the threat intelligence team within Lumen. It is made up of a group of security professionals and data scientists whose mission is to leverage Lumen's global network visibility to both help protect our customers 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, read their blogs.

Read now

Large attacks that make headlines require a lot of investment. Just like legitimate businesses, attackers don't have unlimited funding, talent, or hours in the day. They need to budget their resources and it's not efficient to launch large-scale attacks all the time.

Smaller attacks can also be effective tools for gathering valuable intelligence about a target's defenses, response capabilities, and potential payload. In Q2 2022, Lumen mitigated a 1 Tbps DDoS attack; however, it was preceded by four smaller attacks, which suggests that the threat actors' decisions were rooted in data.

> "In Q2 2022, Lumen mitigated a 1 Tbps DDoS attack that was preceded by four smaller attacks showing that even threat actors need to make data-driven decisions in their initiatives."

All quiet on the Ransom DDoS front

In 2020 and 2021 all you heard about was Ransom DDoS, but in 2022 Lumen observed a decline in extortion requests among our customers. Why would attackers stop leveraging a technique that delivered fairly immediate financial gain?

There could be a few reasons, but we believe more organizations invested in proper backups, better recovery capabilities, and stronger defenses. Additionally, cyber insurance companies have implemented stricter insurance policies to dissuade payments. And at the end of the day, more organizations are just unwilling to pay the ransom.

Now, this isn't to say Ransom DDoS is going away, but as the global community shores up its defenses, we've done our work to make it harder on threat actors to financially gain from victims.

2023 predictions

Attackers will find new resources to leverage

As defenders implement cybersecurity countermeasures to recognize attack traffic patterns, threat actors will look for new ways to launch their attacks. In Q2, we saw attackers use cloud-based, virtual services in a fraudulent way to significantly boost their attack capabilities. They did this by masking their acquisition and control of cloud-based services through compromised hosts or anonymizing services. There have also been reports recently of threat actors using botnets to launch DDoS attacks AND crypto mining activities. As defenders continue to evolve, so do attackers. This will lead to new techniques in the upcoming year.

2 Expansion of the victim pool

With large organizations strengthening their defenses, attackers might begin looking elsewhere to cause chaos. Lumen believes their eyes will turn to the small and mid-sized business space. These organizations might not seem like prime targets, but they typically have fewer cyber defenses and less IT staff to respond to attacks, and they still have critical data and applications they need to protect just like their large counterparts.

3 Timing is everything

It's not new that bad actors are creatures of opportunity. When can they inflict the most damage, and how can they go undetected with no response for the longest time possible? It's every defender's nightmare to get a phone call in the middle of the night saying there's a major attack or breach.

By analyzing the data in our reports we have identified key events during the year when attackers are busy. Thanksgiving, Cyber Monday, and Christmas are always touted as the busy season, but did you know July 4 was the most attacked week in 2021 and 2022? We also saw correlations between attack activity and tax season, and in the weeks leading up to major holidays.

In 2023 organizations need to be prepared during off hours, on holidays, in the weeks surrounding major cultural events, and every other day of the year.

How many DDoS attacks were there?

As with any business, cyberattacks have seasonal ups and downs. Throughout the year, attack trends, styles, techniques, and frequency ebb and flow. In Q4 2022, Lumen mitigated 9,195 attacks — more than any other quarter in 2021 or 2022. This is a 66% increase from Q3 and a 147% increase year over year. On average we mitigated 103 attacks daily, with November 23, 2022 our most attacked day of the year (343 attacks), followed by December 1 and 2 (208 attacks each day).

Lumen mitigated

9,195

DDoS attacks
in Q4 2022

▲66%

from Q3 2022

103

attacks/day

How large are the DDoS attacks?

Largest attack scrubbed

	Dropped bits/s	Dropped pkts/s
Q4 2022	400 Gbps	90 Mpps
Q3 2022	493 Gbps	161 Mpps
QoQ change	↓19%	↓44%
YoY change	↓20%	↑51%

In the first half of the year, Lumen mitigated several large attacks, including 775 Gbps in Q1 and 1.06 Tbps in Q2. However, the median attack size at those times were rather small (0.19 Mbps and .11 Mbps respectively). We have seen a shift lately, with our largest attack sizes getting smaller in the second half of the year, with 493 Gbps in Q3 and 400 Gbps in Q4. On the other hand, our median attack sizes jumped drastically up to 5.76 Gbps. This means that while attackers are still relying on smaller attacks, those small attack sizes are larger than we've previously seen.

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.

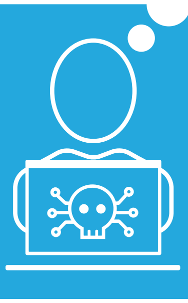
Bandwidth attacks

- The largest bandwidth attack that Lumen mitigated in Q4 was 400 Gbps. This was a 19% decrease quarter-over-quarter and a 20% annual decrease.
- The average attack size was 1.3 Gbps, a 7% decrease from Q3 and a 35% decrease compared to last year.
- In Q2 we mitigated our largest attack to date (over 1 Tbps). Read more on our use case: Anatomy of a Failed DDoS Attack.

Packet rate attacks

- The largest packet rate attack in Q4 was 44% smaller than Q3 coming in at 90 Mpps. However, it's still 51% larger than what we observed in Q4 2021.
- The average packet attack size was 312 Kpps, which was a 28% decrease from Q3 and a 39% decrease compared to last year.

Inside the mind of an attacker



As we've seen with CLDAP and similar attacks, it doesn't take a lot of resources and coordination to make a big impact. The probing "hit-and-run" attacks are more likely to determine how an organization is protecting itself instead of causing operational disruptions. Sadly it doesn't take a lot of coordination or resources to launch big attacks.

Additionally, it's more effective for cybercriminal organizations to leverage existing attack infrastructure and hit victims with smaller-scale attacks than it is to probe defenses first. That way they can back up their "business" decisions with data and have a better understanding of whom to go after with what kind of techniques and what size of attack to get the results they want.

How long are DDoS 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 scrubbed to further minimize downtime.

The data points in this section only portray trends for On-Demand customers, which account for 86% of attacks mitigated in Q4 2022.

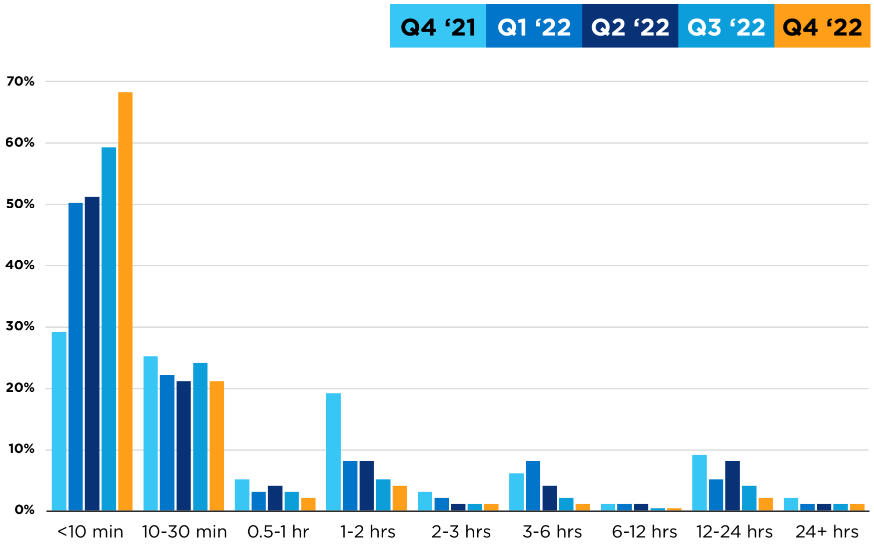
Do I need On-Demand or Always-On mitigation?

	Q4 2022	QoQ change
Median attack duration	7m 26s	↓22%
Average attack duration	1h 19m 42s	↓29%
Longest attack duration	10 days	↑67%

The longest attack period duration we mitigated was ten days. It's important to note that this doesn't mean that there was a single attack that lasted ten days; rather, it means there was an active campaign, which could have contained multiple attacks over time.

We saw a trend in which average and median attack period durations decreased across the year. The median attack period duration decreased by 22% from Q3 to seven and a half minutes. Our most attacked industry was the government sector, and their median attack duration was around five minutes.

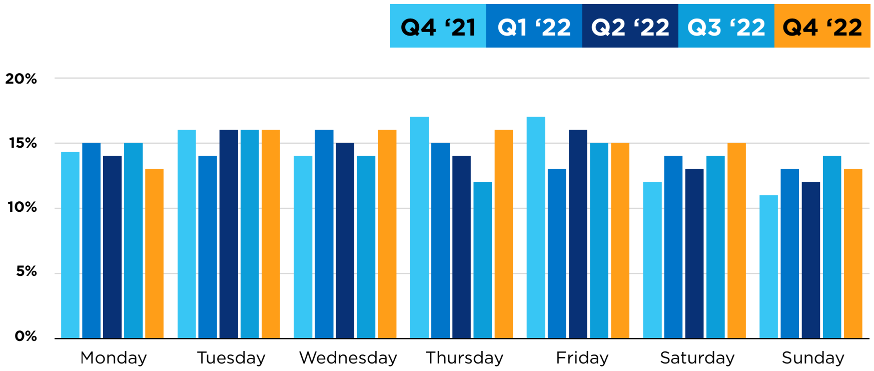
Distribution by duration



> "68% of all attacks on Lumen On-Demand DDoS mitigation customers in Q4 were under 10 minutes. This is a 15% increase and over double what we saw in Q4 2021."

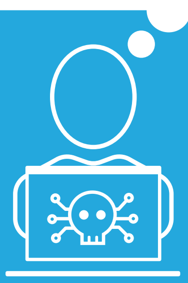
Sixty-eight percent of all attacks on Lumen On-Demand DDoS mitigation customers in Q4 were under 10 minutes. This is a 15% increase and more than double what we saw in Q4 2021. The second most popular attack period duration was 10-30 minutes, representing 21% of activity. Short, quick attacks continue to be heavily leveraged by threat actors.

Distribution by day



Attacks were fairly evenly spread throughout the week. The most popular days in Q4 were Wednesday and Thursday, which each accounted for 16% of activity. This was skewed by a large series of small-scale attacks (343) that occurred on Wednesday, November 23, 2022. Thursday, December 1, 2022, had a large amount of activity as well (208 attacks). Monday, Tuesday and Sunday all were lower activity days each representing 13% of activity.

Inside the mind of an attacker



This quarter's data shows attackers continuing to rely on short and quick-hit attacks. We saw a slew of these attacks target single customers. We had a few customers who were targeted hundreds or even thousands of times over Q4.

Why would an attacker focus so much energy on sending hundreds of 5-minute attacks against a single customer? There could be a few reasons, but a series of small attacks can be just as distracting as one big attack. Victims end up having to spend their resources constantly monitoring attack activity. It's almost like having an alarm go off every 10 muinutes in the morning, and as you try to wake up, you never fully go back to sleep, so the rest is never peaceful.

It could also be a distraction for a more insidious initiative, such as stealing sensitive data. But these short attacks could also mean that they cause the traffic to be scrubbed more often which could cause lag in customer experience if an organization doesn't partner with a DDoS mitigation provider that can handle the capacity or offer Always-On mitigation. Whatever the reason, these minor attacks can have larger consequences for an organization.

What do DDoS attacks look like?

Multi/single-vector attacks

	Q3 2022	Q4 2022	QoQ change
Multi-vector	40%	39%	▼2%
Single-vector	60%	61%	▲2%

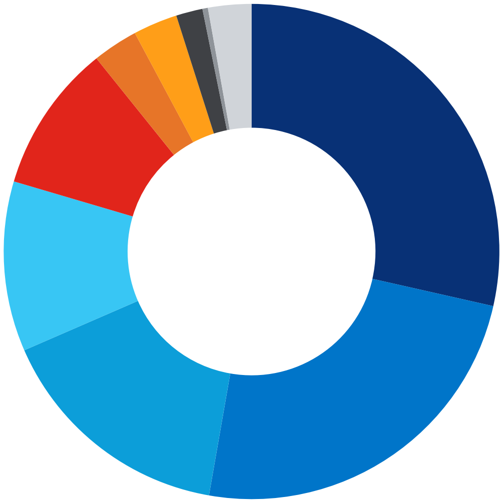
Throughout 2022, Lumen observed multi-vector and single-vector attacks fluctuate slightly, but they usually ended up in a 40/60 split. In Q4 we saw multi-vector attacks accounted for 39% of attacks we scrubbed. They were most prevalent in the Government and Telecom industries. Interestingly, the gaming sector had more single-vector attacks for the first time this year with 58% of activity being single-vector attacks. Usually, the gaming industry has more multi-vector attacks (on average 62%).

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.

Single-vector mitigations

Top single-vector mitigation type breakdown

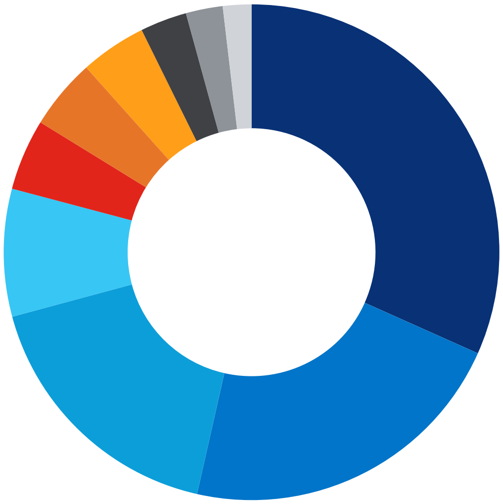


			QoQ
🟦	**DNS**	29%	↑73%
🟦	**TCP SYN**	25%	↑16%
🟦	**Static Filtering**	16%	↓4%
🟦	**UDP**	11%	↓41%
🟥	**Invalid Packets**	10%	↓30%
🟧	**HTTP**	3%	↑5%
🟧	**SIP**	2.9%	↑0.4%
⬛	**Other Volumetric**	1.8%	↓49%
◼	**Per_connection_flood_protection**	0.36%	↓37%
⬜	**Other**	2.87%	N.A.

When looking at the breakdown of single-vector mitigation types, Domain Name System (DNS) amplification attacks overtook our reigning champ, TCP SYN. DNS amplification attacks became more popular in the second half of 2022 and in Q4 account for 29% of activity, which is a 73% quarterly increase and a drastic spike compared to Q4 2021 when it only accounted for 1% of activity.

TCP SYN Flooding was still used frequently, accounting for 25% of activity, which was a 16% increase from Q3 and an 89% increase from Q4 2021. This continues to be a proven method for attackers to use because it does not require a large volume to disrupt the availability of service for targeted devices. In other words, a smaller attack can pack a bigger punch.

Static Filtering accounted for 16% of activity in Q4, which is a 4% decrease quarter-over-quarter. Static filtering countermeasures are typically done on items such as ports and protocols. These statistics also include known bots and abused reflectors as discovered by Black Lotus Labs, which provided initial mitigation against attacks.



Multi-vector mitigations

Top multi-vector mitigation type combinations

			QoQ
🟦	**DNS, TCP SYN**	21%	↑50%
🟦	**DNS, TCP SYN, Static Filtering**	14%	↑72%.
🟦	**DNS, Static Filtering**	11%	↑138%
🟦	**TCP SYN, Static Filtering**	5%	↑7%
🟥	**UDP, Static Filtering**	3%	↑15%
🟧	**Other Volumetric, UDP, Static Filtering**	3%	N.A.
🟨	**Other Volumetric, UDP**	3%	N.A.
⬛	**Invalid Packets, UDP**	2%	↓11%
◼	**Invalid Packets, Static Filtering**	2%	↓35%
⬜	**Invalid Packets, UDP, Static Filtering**	1%	↓25%

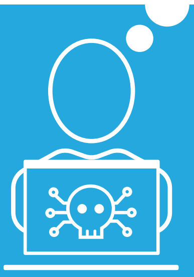
The nature of multi-vector attacks means they require multiple countermeasures to mitigate, making them more difficult to prevent. For proper mitigation, organizations should consider combining DDoS Mitigation with Application Protection to enable a holistic defense strategy.

Learn more

We finished out the year with DNS amplification combined with TCP SYN Flooding being the most leveraged multi-vector attack. This combination accounted for 21% of activity in Q4, which is a 50% increase compared to Q3 and a 73% annual increase. DNS Amplification is used because DNS is essential and cannot be turned off or blocked, and it provides a degree of anonymity to attacks. TCP SYN is spoofed, providing an added level of anonymity, and can target service ports that also cannot be blocked either. At the end of the day, both methods combined require more sophistication than a "deny" rule to defend against.

Additionally, we saw DNS, TCP SYN and Static Filtering used together in 14% of multi-vector attacks which is a 72% increase from Q3. We also saw a variation of this with the combination of DNS and Static Filtering accounting for 11% of activity (more than double what we saw in Q3).

Inside the mind of an attacker

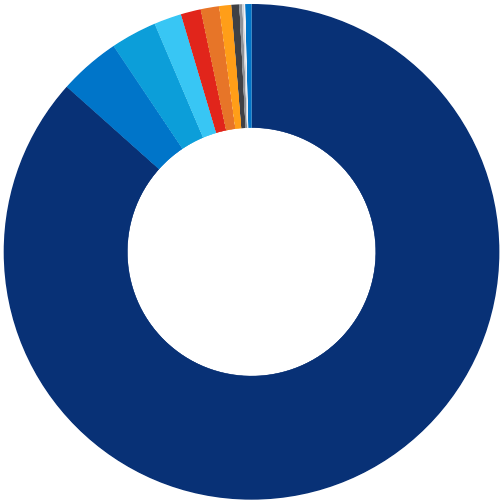


We've all been saying for years that attacks are getting more complicated and complex. And while that remains true on a large scale, bad actors are using simpler attacks as well. As discussed above, we've seen DNS amplification being used more frequently which could be because DNS is an essential service, and DNS traffic is expected. It can be easier to fly under the radar if you're using something an organization thinks they should be seeing versus a UDP amplification attack which is noisier but has been around long enough that organizations are beginning to filter out that traffic.

Like CLDAP reflection, DNS amplification attacks take advantage of servers that are open to the public internet and use them to send DDoS traffic to an intended target. They're hard to defend against because the attacker is using someone else's server to send traffic to the victim.

Who is being attacked?

Largest 1,000 attacks by industry



Telecommunications	87%
Software & Technology	4%
Gaming	3%
Government	2%
Hosting	1.3%
Finance	1.2%
Banking	0.8%
Education	0.5%
Media & Entertainment	0.2%
Utilities	0.1%
Business Services	0.1%
Other	0.4%

Of the 1,000 largest attacks Lumen mitigated, 97% targeted these top five verticals (in order): Telecommunications, Software and Technology, Gaming, Government, and Hosting.

It is important to note that a single government customer represented 60% of all the attacks Lumen mitigated in Q4; they were targeted with over 5,500 attacks. The customer also experienced the largest attack we mitigated in Q4 — 400 Gbps — but more were small, short attacks averaging 5 minutes in duration. Forty-two percent of attacks used DNS and 34% used TCP SYN. We observed large concentrations of attack activity on November 23, 2022 (305 attacks), and December 4, 2022 (174 attacks).

Telecommunications

87% of the largest 1,000 attacks

1,870 total attacks against vertical

Largest bandwidth attack: **365 Gbps**

Longest attack period duration: **6 days**

69% multi-vector attacks

Largest packet-based attack: **90 Mpps**

Software and Technology

4% of the largest 1,000 attacks

258 total attacks against vertical

Largest bandwidth attack: **91 Gbps**

Longest attack period duration: **5 days**

74% single-vector attacks

Largest packet-based attack: **71 Mpps**

Gaming

3%
of the largest
1,000 attacks

146
total attacks
against vertical

Largest
bandwidth attack:
54 Gbps

Longest attack
period duration:
4 days

58%
single-vector
attacks

Largest
packet-based attack:
28 Mpps

Government

2%
of the largest
1,000 attacks

5,795
total attacks
against vertical

Largest
bandwidth attack:
400 Gbps

Longest attack
period duration:
3 days

65%
single-vector
attacks

Largest
packet-based attack:
50 Mpps

Hosting

1.3%
of the largest
1,000 attacks

79
total attacks
against vertical

Largest
bandwidth attack:
18 Gbps

Longest attack
period duration:
5 days

68%
single-vector
attacks

Largest
packet-based attack:
37 Mpps

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

LUMEN®

What is the cost of a DDoS attack?

The biggest question you might have coming out of this report is: “okay so what’s the impact?” The financial impact of DDoS attacks can vary based on the organization. The cost of a DDoS attack is determined by hours of downtime, the number of IT security staff you have dedicated to security incidents, the number of customer complaint communications you may receive, and how much revenue is tied up in your websites and applications.

But let’s take a look at a use case — a Software and Technology company that does $2 billion in total revenue, and about $500 million of that comes from online motions. They have a smaller size IT team with two people dedicated to fixing security issues (such as responding to DDoS attacks). During a breach, they will receive about 25 customer support calls per hour.

Based on data from our reports, we expect a company like this to be targeted 13 times annually, with an average downtime of 19 hours per attack.

We anticipate the total final loss to be $20,688,500.* We found that revenue would be negatively impacted by a little over $14 million, the cost impact from IT operations and customer support to be over $64,000, and the negative impact to the organization to be $6.5 million. This would be for all 13 attacks, however, after the first attack using our example the cost would be $1.6 million, and an organization would likely invest in DDoS mitigation services to mitigate future financial exposure. But these are real numbers that can financially devastate an organization.

If you’re interested in learning how your business would be impacted by as DDoS attack, check out our attack cost calculator.

* The DDoS cost calculator tool is provided for illustration purposes only and does not constitute an offer or guarantee for services or savings. The tool uses Lumen data along with industry data and assumptions as of September 2022 as well as the data you input to calculate and estimate alerts and their impact. Any change in data will result in a change to the information provided in the report.

Final thoughts from Lumen

As we close out 2022 and look into 2023, there's one thing that we know to be true — attackers will continue to evolve. Every time we appear to successfully defend against a technique, attackers return with a new attack vector. The world of cybersecurity is always changing, but one thing remains the same: the best defense is to have a solid strategy in place.

Recommendations:

- Nowadays, 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-layer attacks will ensure your critical business functions stay up and running – even if you are under an active attack. Consider deploying additional application layer defenses using Web Application Firewalls, API protections and Bot Management solutions and couple those with application acceleration solutions to make applications more responsive for your customers.
- 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 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 named 2022 Overall Network Security Solution Provider of the Year by *Cybersecurity Breakthrough*.

CYBERSECURITY BREAKTHROUGH AWARD 2022

NETWORK SECURITY SOLUTION PROVIDER OF THE YEAR

Read our exciting news!

Methodology

Data in this report is from the timeframe of October 1, 2022 through December 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 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

This information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. 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.

LUMEN®