

REPORT

Lumen Quarterly DDoS Report

Q3 2022

Executive Summary

The only consistent thing about the threat landscape is its inconsistency. Security teams have their work cut out for them and it's not getting any easier. The news reports about the ongoing slew of cyberattacks are enough to keep anyone awake at night.

The purpose of our Quarterly DDoS Reports is to provide you an overview of the DDoS attacks we mitigate and put them into context for you. We seek to help you answer 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



Attackers are exploiting vulnerabilities in essential services to **amplify attacks up to 70 times in size.**

2



Holidays are ideal for adversaries — they're looking to take advantage of potentially understaffed IT and security teams.

3



The trend in which actors deploy smaller and shorter attacks to evaluate organizations' defenses — known as **"hit-and-run" style attacks** — continues.

Numbers you need to know for Q3 2022:



DDoS attacks increased
21%
quarter over quarter.



Multi-vector attacks are again on the rise, accounting for
40%
of attacks.



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

Table of Contents

Key findings for Q3 2022	4
Threat alert from Lumen: Attackers using CLDAP to amplify DDoS attacks up to 70 times	5
How many DDoS attacks were there?	8
How large are DDoS attacks?	8
How long are DDoS attacks lasting?	9
What do DDoS attacks look like?	11
Who is getting DDoS attacked?	14
Final thoughts from Lumen	16

Key findings for Q3 2022

- The number of attacks mitigated increased by 21% compared to Q2 2022 and decreased by 23% annually.
- The largest bandwidth attack we scrubbed in Q3 was 493 Gbps, which was half the size of the largest attack we mitigated in Q2.
- The largest packet rate-based attack we scrubbed in Q3 was 161 Mpps, which was a 35% decrease compared to Q2.
- The longest DDoS attack period we mitigated for an individual customer lasted six days.
- 83% of attack periods targeting our On-Demand DDoS customers were less than 30 minutes.
- Tuesdays were the busiest day for attacks and Thursdays were the slowest.
- 40% of all mitigations were multi-vector, and the most common combination used DNS and TCP SYN countermeasures.
- The most common type of single-vector mitigation — accounting for 21% of the total — was TCP SYN flooding
- The top three targeted verticals in the 500 largest attacks were: Telecommunications, Gaming and Software and Technology.

Threat alert from Lumen: Attackers using CLDAP to amplify DDoS attacks up to 70 times

“CLDAP is an attractive reflection vector because it carries a bandwidth amplification factor of 56 to 70 times the original request.”

What does UDP mean?

User Datagram Protocol — UDP is a way for low-latency information to pass between applications. It's faster than TCP and can therefore be used for time-sensitive or real-time communications like VoIP calls and video playback.

For years the security industry has warned that DDoS attacks are getting more sophisticated. This isn't a scare tactic — it's true. When it comes to DDoS attacks, particularly reflective DDoS attacks, you must not only prepare to withstand the attack, but you must also be aware of potential gaps in your defenses that could make you an unwitting participant. In this section, we will breakdown a powerful tactic involving the abuse of a protocol that's essential in Microsoft environments. It's something that Lumen's threat intelligence team — [Black Lotus Labs®](#) — is actively tracking. We will also provide advice to help you protect your organization from this potentially serious cyberthreat.

What is CLDAP?

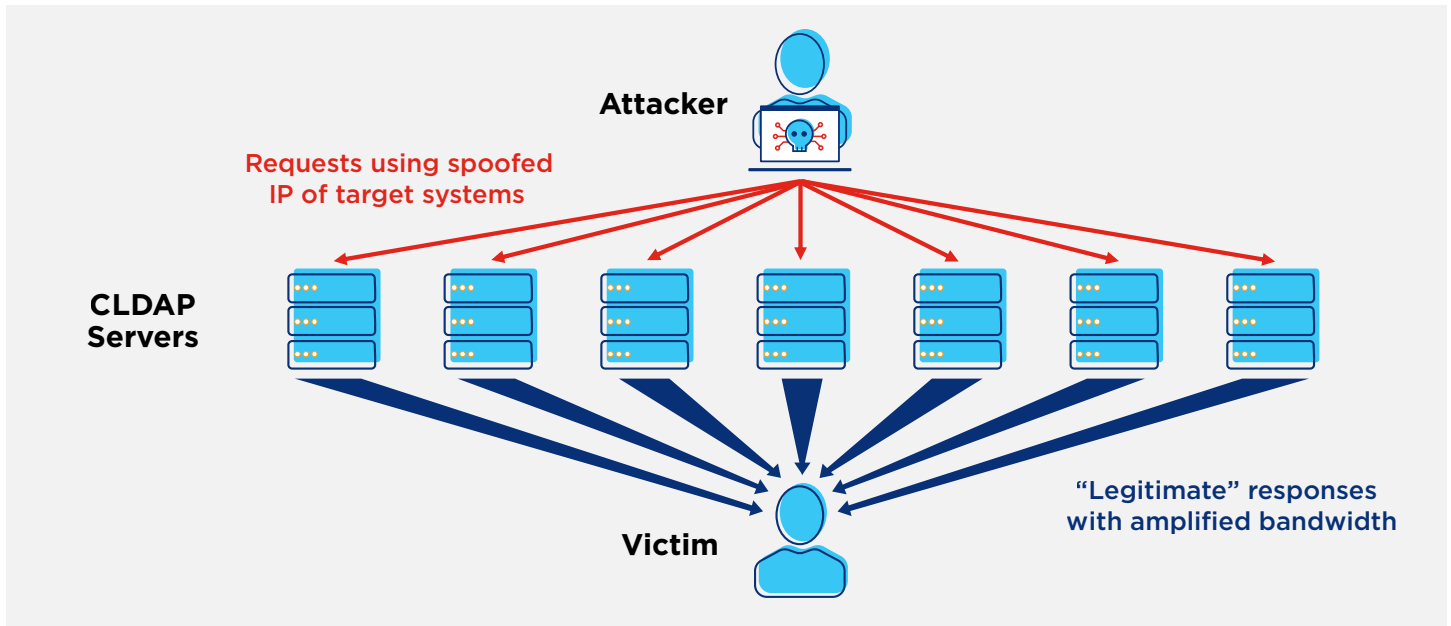
CLDAP stands for Connectionless Lightweight Directory Access Protocol. LDAP is an industry-standard protocol for interacting with a directory service over an IP network. Your organization has directory information — things like usernames, passwords, email addresses and employee names — that needs to be stored somewhere. At the same time, your company uses business applications that need some way to read that information. LDAP allows business applications to query user information.

The connectionless part (the “C” in CLDAP) comes from those requests for information being done over UDP, a best-effort protocol that, unlike TCP, does not require confirmation of a connection before sending or receiving information. While many directory services implement full LDAP over TCP, Microsoft Active Directory (AD) is a notable exception that also uses CLDAP. The problem is that, when misconfigured to be exposed to the internet, a CLDAP service is vulnerable to cyber attackers leveraging it to launch reflective DDoS attacks. Given that AD is a widely used, essential element of any Microsoft network, it's critical that CLDAP services are properly configured. Black Lotus Labs intelligence indicates that this best practice is frequently not followed, and the number of CLDAP reflectors is on the rise.

How and why are attackers using CLDAP?

We covered [UDP reflection](#) last year in our [Q3 DDoS Quarterly Report](#), but to recap: a reflection attack is when an actor uses the target system's IP as the source IP on a request sent to a UDP service, such as CLDAP. Lacking any connection information, UDP will honor the bogus return address and fire its response to the target system.

In addition to directing traffic to the target, this also hides the true IP of the attacker — a strong nice-to-have feature for DDoS operators. Additionally, many UDP services return a response payload much larger than the submitted request payload, thus amplifying the attack traffic without needing more attacker-owned resources. Obviously, threat actors are particularly fond of these reflection vectors because they add potency without requiring additional investment by procuring infrastructure or cultivating a [botnet](#).



For what it's worth, CLDAP is an attractive reflection vector because it carries a bandwidth amplification factor of 56 to 70 times the original request. The May 2021 DDoS attack targeting Belnet, one of the ISPs for the Belgian government, was at one point comprised almost entirely of reflected CLDAP traffic. More recently, the Russian aligned Killnet hacktivist organization has been observed leveraging [CLDAP reflection](#), among other DDoS attack vectors, against its targets. What's more, in recent research, [Black Lotus Labs reported](#) that the number of CLDAP reflectors available on the internet has increased more than 60% over the past year.

“The number of CLDAP reflectors available on the internet has increased more than 60% over the past year.”



How can you stop making it easy for attackers?

The most effective way to prevent CLDAP reflection attacks is to ensure CLDAP is properly configured to prevent abuse. Even though you're not the one being attacked, you still don't want your network or devices to be used to attack someone else, nor do you want to foot the bill for Gigabits of attack traffic emitting from your service.

In addition, Black Lotus Labs has observed that exposed CLDAP services are often infected with malware. Once an adversary has access to your system, you're open to a myriad of attacks, from data theft to crypto mining and ransomware. There are a few things you can do, however, to minimize your risk:



1 **Check your CLDAP configurations.** You most likely don't need to have CLDAP services open to the public internet.



2 **Monitor your logs.** Watching your network bandwidth and usage can help you determine if your exposed CLDAP service is being abused or if you're part of a botnet.



3 **Protect and limit your publicly accessible services.** For services prone to reflection, the network security team at your organization should restrict in-bound traffic and possibly rate-limit these services as well. This keeps your networks from generating reflected attack traffic.

You can also prevent initiation of reflection by preventing the egress of spoofed traffic from your networks. Please also consider applying some sort of egress filtering such as RPF to stop this spoofed traffic as close to the source as possible.

Lumen Black Lotus Labs is leading the charge on CLDAP reflection attacks

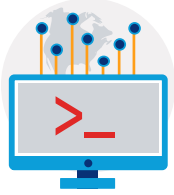
Our threat intelligence team is taking steps to help the internet community at large defend against CLDAP reflection attacks. Lumen has one of the largest, most deeply peered and connected networks, which means we have unparalleled threat visibility. By observing commonly used attack patterns, we can create validators to track their behavior and flag if those patterns are being used.

While CLDAP attacks aren't new, we see them employed in DDoS attacks every day. Worse – we see that the number of reflectors is on the rise. This is why we alert the owners of vulnerable CLDAP reflectors in the Lumen IP space, and we are working to help disrupt attacks by blocking long-lived CLDAP reflector traffic from traversing the Lumen global backbone.

If you're interested in learning more about CLDAP reflection, read our research from Black Lotus Labs.

[CLDAP Reflectors on the Rise Despite Best Practice](#)

How many DDoS attacks were there?



Lumen mitigated
5,547
DDoS attacks
in Q3

↑21%
from Q2

63
attacks/day

As with many trends, DDoS attacks experience seasonality, so there will be times when attacks are more frequent. We mitigated 5,547 attacks in Q3 — a 21% increase compared to Q2. On average, we mitigated 63 attacks daily, with July 5 and July 4 experiencing the most attacks (241 and 233, respectively).

How large are DDoS attacks?

Largest attack scrubbed

	Dropped bits/s	Dropped pkts/s
Q3 2022	493 Gbps	161 Mpps
Q2 2022	1062 Gbps	246 Mpps
QoQ change	↓54%	↓35%
YoY change	↓19%	↓36%

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 Q3 was 493 Gbps. This is a 54% quarter-over-over decrease and a 19% annual decrease. It's important to note, however, that we mitigated our largest attack to date (over 1 Tbps) in Q2. [Learn more about the failed 1 Tbps attack.](#)

The average attack size was 1.4 Gbps, which is an 18% decrease from last quarter. This could be due to attackers using small attacks to probe organizations to detect whether they have DDoS mitigation.

Packet rate attacks

The largest packet rate attack in Q3 was 35% smaller than Q2, coming in at 161 Mpps. Despite the size being smaller than Q2, it was larger than Q1 2022 or Q4 2021.

The average attack size was 434 Kpps — a 12% decrease from last quarter.

Misconception #1: A 1 Gbps attack isn't a big deal.

Let's be honest — you're probably not going to be hit with the largest attack on record. While DDoS attacks, in general, are becoming larger, our data shows attackers typically 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 all represent customers who have DDoS mitigation services. So, attackers could potentially see that our customers have protection and move along to find someone else with a more vulnerable security posture.

Another potential reason actors are launching smaller attacks is to 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 posture is current will help ensure that if a larger attack comes your way, your operations are not affected.

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 78% of attacks mitigated in Q3 2022.

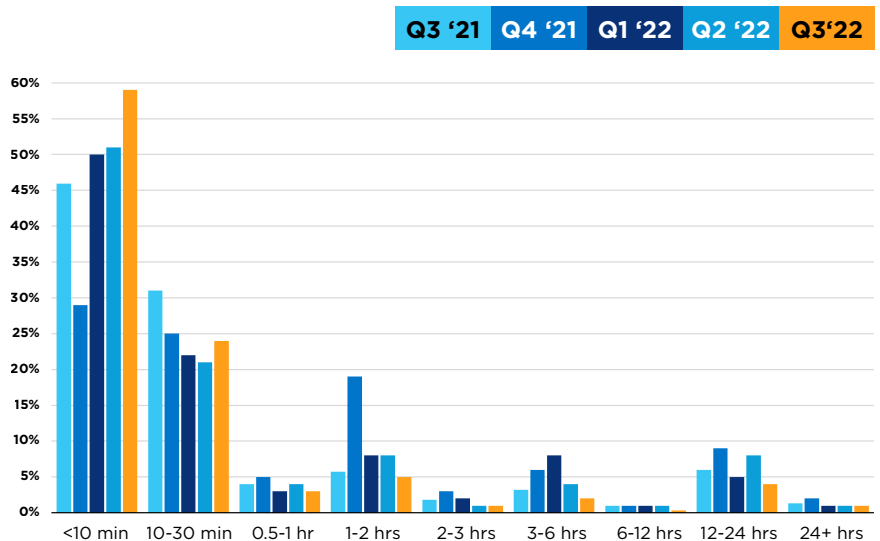
Do I need On-Demand or Always-On mitigation?

	Q3	QoQ change
Median attack duration	9m 33s	↓5%
Average attack duration	1h 56m 53s	↓46%
Longest attack duration	6 days	↓71%

The longest attack period duration we mitigated was six days. This does not mean there was a single attack that lasted six days; rather, it means there was an active campaign, which could have contained multiple attacks over time. There were DDoS campaigns against both the government sector and the software and technology sector that lasted six days.

The average attack period duration decreased by 46% quarter over quarter, ending up just shy of two hours. The software and technology industry, however, experienced an average attack period duration of around 22 hours — the highest of all verticals.

Distribution by duration

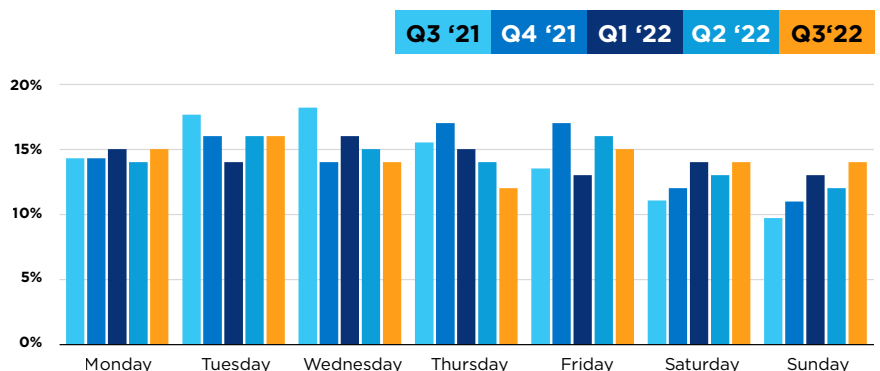


“There were DDoS campaigns against both the government sector and the software and technology sector that lasted six days.”

Nearly 60% of all attacks on Lumen On-Demand DDoS mitigation customers lasted less than 10 minutes. This is a 16% increase quarterly and a nearly 30% increase annually. The second most common attack-period duration was 10-30 minutes, representing 24% of activity. We spoke to this trend in our Q2 2022 report — the bad actors use quick hits to scope out defenses for potentially larger attacks, or they use this as a distraction for bigger, nastier initiatives.

We saw decreases across every other time frame from 30 minutes to more than 24 hours.

Distribution by day



Attacks continue to occur evenly throughout the week. The most popular day is Tuesday, which accounted for 16% of the activity. Thursday had the least amount of activity this quarter accounting for only 12% of the total. This is slightly unusual, considering weekends typically have the lowest activity. In fact, Sundays saw a 14% increase in activity in Q3.

Misconception #2: A short attack won't affect my organization.

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. You should think of time in terms of the monetary impact to your operations. 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 surprise 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

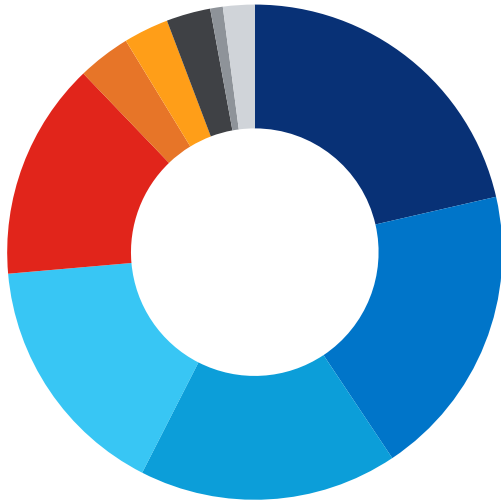
	Q2	Q3	QoQ change
Multi-vector	38%	40%	↑5%
Single-vector	62%	60%	↓3%

Lumen observed a rise in multi-vector DDoS attacks by 5% quarterly; however, single vector attacks still lead, accounting for 60% of activity. While multi-vector attacks accounted for 40% of the attacks we scrubbed, they were more prevalent in the telecommunications (74%) and gaming (69%) verticals.



Single-vector mitigations

Single-vector mitigation type breakdown



		QoQ
TCP SYN	21%	↓22%
UDP	19%	↓14%
DNS	17%	↑420%
Static Filtering	16%	↓24%
Invalid Packets	14%	↓15%
Other Volumetric	3%	↑70%
SIP	2.9%	↑59%
HTTP	2.9%	-
TCP RST	0.81%	↑21%
Other	2.05%	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 21% of activity. This was a 22% decrease compared to Q2 when TCP SYN accounted for 27% of mitigations. 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.

UDP-based amplification decreased 14% quarterly and is on track with what we observed one year ago, accounting for 19% of activity. 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 as the campaign progresses and becomes exponentially larger.

Domain Name System (DNS) amplification attacks spiked drastically this quarter — more than any other activity we've seen in past reports. Quadrupling in activity, this attack vector accounted for 17% of mitigations. 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.

As we predicted in our last quarterly report, we saw an increase in SIP attacks. They accounted for 3% of activity, which is a 59% increase from last quarter and higher than our previous quarterly reports. 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	14%		▼32%
DNS, TCP SYN, Static Filtering	8%		N.A.
TCP SYN, Static Filtering	5%		▼22%
DNS, Static Filtering	5%		N.A.
TCP SYN, UDP, Static Filtering	4%		N.A.
TCP SYN, UDP	3%		▲69%
UDP, Static Filtering	3%		N.A.
Other Volumetric, TCP SYN, UDP, Static Filtering	3%		N.A.
Invalid Packets, Static Filtering	2%		N.A.
Invalid Packets, UDP	2%		N.A.

For the third quarter in a row, DNS combined with TCP SYN was the most popular type of multi-vector attack, accounting for 14% of activity in Q3. While this is a decrease from last quarter, it is a 15% increase year over year. DNS Amplification is used because DNS is essential and cannot be turned off or blocked, 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. So both methods combined require more sophisticated than a “deny” rule to defend against.

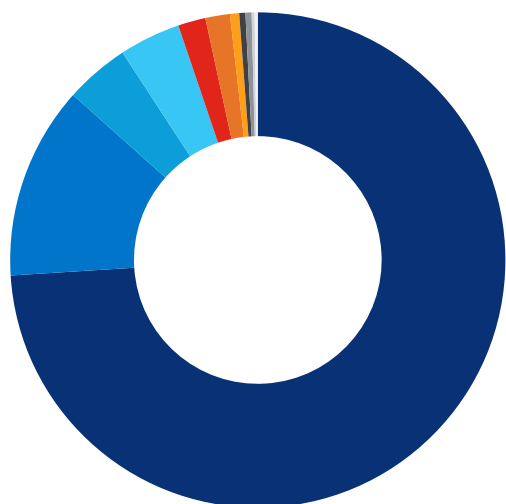
The second most popular multi-vector attack combination included DNS, TCP SYN and Static Filtering. This was the first time we’ve seen this combination since last year in Q3 and it’s double what we’ve previously seen.

Misconception #3: 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. But what if your network could be used as a line of defense? Lumen has one of the largest networks in the world and we use that backbone as a threat sensor. Leveraging Black Lotus Labs’ threat intelligence, we integrate our knowledge and tracked behaviors into our security solutions via Rapid Threat Defense, which automatically blocks and disrupts DDoS attacks in the network instead of waiting for attacks to reach customers.

Who is getting DDoS attacked?

Largest 500 attacks by industry



Telecomm	74%
Gaming	13%
Software & Technology	4%
Government	4%
Finance	2%
Hosting	2%
Consulting	1.00%
Manufacturing	0.40%
Education	0.40%
Healthcare	0.20%
Business Services	0.20%

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

It was interesting to note that a single government customer was targeted more than 2,200 times, accounting for almost 40% of all the attacks we mitigated in Q3.

The average attack size was 95 Mbps, and the attacker mostly leveraged single-vector techniques — specifically TCP SYN. While most of these attacks were spread throughout the quarter, there was a noticeable increase on July 4 and July 5. This could have been the result of threat actors looking to strike when the target's IT and security teams were likely out of the office for the holiday.

Telecommunications



74%

of the largest
500 attacks



1,384

total attacks
against vertical



Largest
bandwidth attack:
327 Gbps



Longest attack
period duration:
5 days



74%
multi-vector
attacks



Largest
packet-based attack:
88 Mpps

Gaming



13%

of the largest
500 attacks



177

total attacks
against vertical



Largest
bandwidth attack:
76 Gbps



Longest attack
period duration:
3 days



69%
multi-vector
attacks



Largest
packet-based attack:
12 Mpps

Software and Technology



4.2%

of the largest
500 attacks



319

total attacks
against vertical



Largest
bandwidth attack:
493 Gbps



Longest attack
period duration:
6 days



80%
single-vector
attacks



Largest
packet-based attack:
161 Mpps

Government



4%

of the largest
500 attacks



2,326

total attacks
against vertical



Largest
bandwidth attack:
30 Gbps



Longest attack
period duration:
6 days



65%
single-vector
attacks



Largest
packet-based attack:
43 Mpps

Finance



1.8%

of the largest
500 attacks



206

total attacks
against vertical



Largest
bandwidth attack:
328 Gbps



Longest attack
period duration:
4 days



82%
single-vector
attacks



Largest
packet-based attack:
29 Mpps

Misconception #4: 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 5,500 attacks in Q3. In addition, as we've stated before, attackers continue to use quick, hit-and-run style attacks to disrupt operations, avoid detection and test your defenses. Every organization is a target nowadays 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](tel:800-871-9244).

Final thoughts from Lumen

When it comes to cybersecurity, the desire to stay one step ahead in an ever-changing landscape can keep you up at night. 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 help ensure 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?

**Lumen named 2022
Overall Network
Security Solution
Provider of the Year
by *Cybersecurity
Breakthrough*.**



[Read our exciting news!](#)

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.



Methodology

Data in this report is from the timeframe of July 1, 2022 through September 30, 2022.

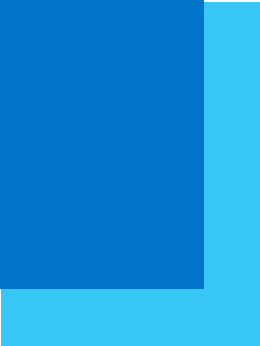

Scrubbed attacks are defined as either:

- 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