REPORT

Lumen Quarterly DDoS Report

Q4 2021

LUMEN® TECHNOLOGIES

Introduction

Another year has come to a close, and with that it's time to reflect on 2021. It was a busy year for everyone — especially those who work tirelessly to keep the internet clean. We watched as major attacks took over headlines and disrupted not just businesses, but communities at scale. And as soon as one piece of malicious infrastructure is disrupted, another one pops up — like an intense game of whack-a-mole.

In our Lumen Quarterly DDoS Report for Q4 2021 you'll learn:

- Security predictions for the upcoming year
- Attack size, length, and frequency
- DDoS attack vectors
- Targeted industries

For this report, we examined intelligence from Black Lotus Labs® and data from the Lumen® DDoS Mitigation platform to develop our findings, which both reinforced and expanded on broader trends. Here's a quick glimpse at DDoS attack trends Lumen observed this year:

Total number of attacks mitigated:

20,585

Average Mirai/Gafgyt C2s tracked per quarter:

800

Average Mirai/Gafgyt bots tracked per quarter:

200,000

Largest bandwidth attack size:

612 Gbps

Longest attack period duration:

14 days

Most common single-vector attack countermeasure:

Static Filtering

Three most attacked verticals:

Telecoms

Software and Tech

Government

LUMEN® TECHNOLOGIES

Table of Contents

LUMEN® TECHNOLOGIES

Key Findings for Q4 2021

IoT DDoS Botnets

- There was a 56% quarterly increase in unique C2s tracked for pervasive DDoS botnets Gafgyt and Mirai.
- The average lifespan of Gafgyt C2 was 32 days, while Mirai's C2 average lifespan was 12 days.
- Lumen tracked 1,724 C2s globally. The countries with the most C2s were (in order): United States, The Netherlands and Canada.
- Lumen observed a 17% quarterly increase in the number of DDoS botnet hosts globally. The countries with the most DDoS botnets were (in order): Mexico, Brazil and India.

DDoS Attack Trends

- The number of attacks we mitigated decreased by 48% compared to Q3.
- The largest bandwidth attack we scrubbed in Q4 was 499 Gbps, which is a 27% decrease quarter-over-quarter.
- The largest packet rate-based attack we scrubbed in Q4 was 60 Mpps, which was a 76% decrease from Q3.
- The longest DDoS attack period we mitigated for an individual customer lasted 5 days.
- 54% of attack-period durations were over 30 minutes when looking at our On-Demand DDoS customers.
- Multi-vector mitigations represented 35% of all DDoS mitigations, with the most common combination using DNS and TCP SYN countermeasures.
- UDP amplification was the most common single-vector mitigation type, accounting for 29% of DDoS mitigations.
- The top three targeted verticals in the 500 largest attacks in Q4 were: Telecom, Gaming, and Software and Technology.

What Can We Expect Out of 2022?

Before we dive in, let's take a moment to celebrate making it through another year, despite numerous challenges. Looking at what happened around the world, we saw another year in which a huge portion of the workforce continued to work remotely. And in 2021, we saw many high-profile cyberattacks hit the news and, in some cases, cause public unrest in the United States. While it appears that things are returning to some sense of normalcy, one thing is certain: cyberattackers will continue to keep us on our toes.

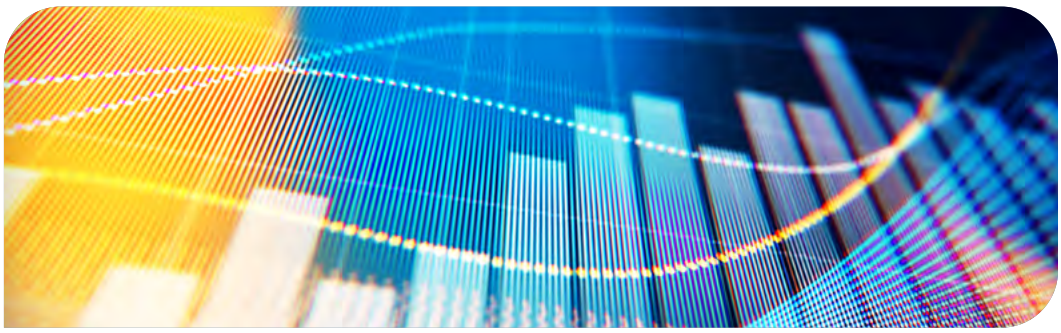
2021 Trends

1. **Beware of ransom DDoS:** As threat actors look for financial gain from their activities, they frequently relied on ransom DDoS attacks. There were spikes throughout the year where ransom DDoS was the primary mode of attack for bad actors. Specifically, we observed a lot of activity from May-July. Additionally, while ransom notes primarily demand Bitcoin for payments, there were several demands for payments to be made in Monero, instead.

   For a deeper dive into ransom DDoS activities, read our report from Q2. Download report

2. **Voice providers are a prime target:** In Q3 we observed a number of voice providers come under attack. Traditionally, VoIP services haven't seen the kind of volumetric attacks that were causing significant impact to some providers. However, after Q3, the main attack infrastructure that was targeting them was disrupted.

3. **Reflection attacks continue to be an attack vector of choice:** In 2021 attackers used reflection-style attacks because such an attack can become very large with very little effort on the part of the attacker. Whether it's CLDAP, NTP, DNS, SSDP, or other protocols susceptible to amplified reflection attacks, hackers are relying on this vector category to cause significant damage. Read our Q3 report for an in-depth review of spoofed reflection attacks. Download report



2022 Predictions

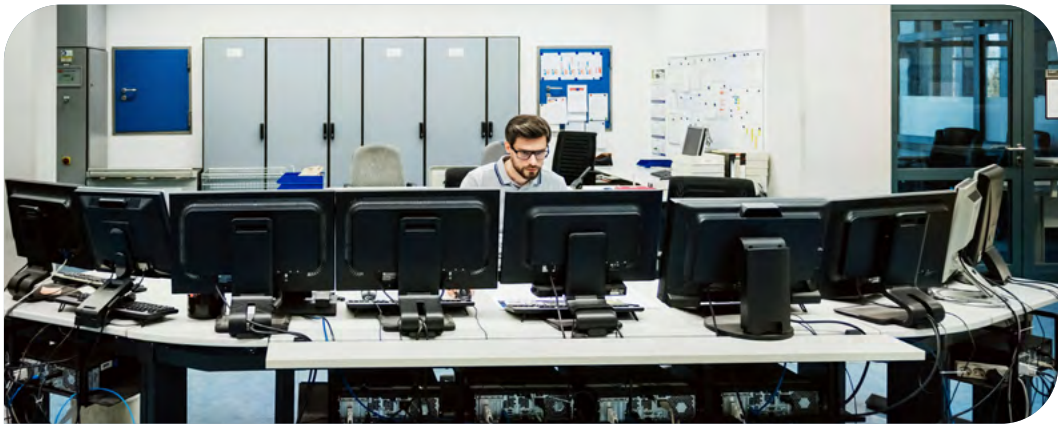
1. **Expect spikes and lulls in ransom DDoS:** Lumen expects that some sort of seasonality will begin to appear with ransom DDoS attacks. We'll likely have some dry periods followed by a flurry of activity with attackers opting for a shock and awe campaign. Major attacks will also inspire others, and we predict there will be copycat activity.

2. **There will be an increase in more sophisticated, multi-vector attacks:** We already saw an increase in attack complexity throughout 2021, and that will continue in 2022. You can expect to see the largest volumetric attack ever seen next year because botnets continue to grow in size and complexity every year. And similar to a Hydra, as soon as you cut off one piece of suspected infrastructure, another one pops up. There will also be a growth in Layer 7 attacks increasing the need for web application protection and bot management to defend new application-driven revenues.

3. **Increased collaborative disruptions of crimeware in the midst of increased nation-state activity:** As nation-state attacks are becoming increasingly more prevalent (not just to DDoS specifically), and as industry and governments continue to collaborate as they did with several attempted takedowns such as Emotet last year, we anticipate these types of collaborations will bear more fruit.

   Given the political landscape in Eastern Europe, we expect to see an increase in nation-state sponsored attacks in 2022. In addition, Western nations should be prepared to defend against direct campaigns or collateral damage. Campaigns are expected to include, but not be limited to, ransomware, DDoS and attacks against critical infrastructure.

   Black Lotus Labs and Lumen will continue to do our part in keeping the internet a safe place; read one of our recent blogs to learn about the latest threats and trends: New Konni Campaign Kicks off the New Year by Targeting Russian Ministry of Foreign Affairs.



IoT DDoS Botnets: Lumen remains vigilant

Family	Unique C2s tracked	Unique attack victims per family	Average lifespan of a C2 (in days)
Gafgyt	507 ▲45% QoQ	1,117	36 ▼5% QoQ
Mirai	480 ▲69% QoQ	21,140 ▼5% QoQ	12 ▼42% QoQ

The two predominant DDoS IoT botnet families that Black Lotus Labs tracks, Gafgyt and Mirai, continue to wreak havoc with hundreds of C2s dispersed across the globe. We have tracked these families for years because they continue to prevail, either with slight modifications or new infrastructures continuing to pop up. Q4 data was on par with what we have found in previous quarters; however, due to the shifting nature of botnet activity, we expect to see those figures ebb and flow.

Overall, there was a 56% increase in the total unique C2s tracked, with Mirai accounting for the majority the quarter-over-quarter shift, rising 69% since Q4.

We define “victims” as the number of unique IPs against which we observed the C2s launching DDoS attacks. Combined, there were more than 22,200 victims across both botnet families, which is on par with our quarterly average for the year 2021.

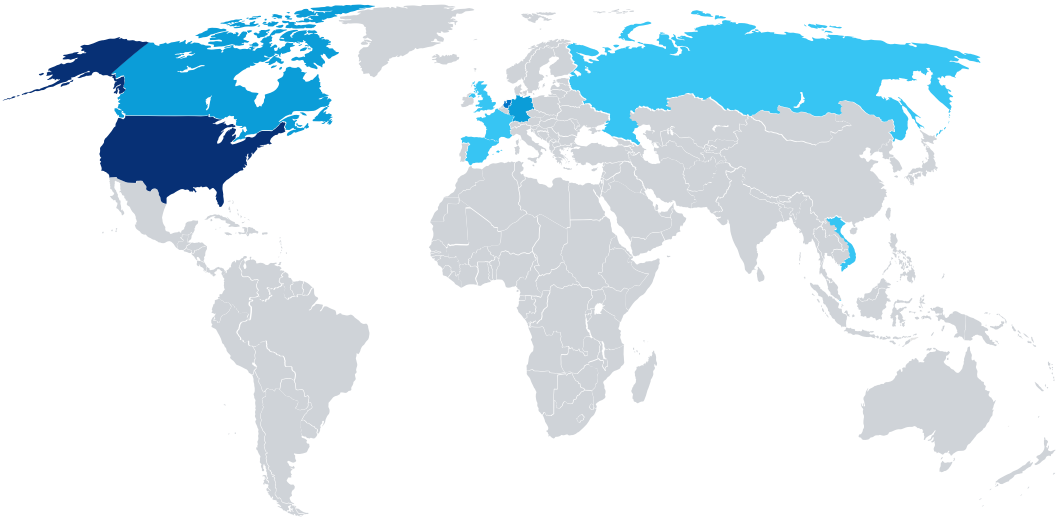
One of the bad actors’ goals is to cultivate reliable infrastructure they can use for their own attacks or to rent as a service to other actors for temporary use. That means they’re aiming to keep those infrastructures alive as long as possible. This quarter, Gafgyt’s lifespan was in line with what we saw in other quarters this year, with a slight decrease of 5%. Mirai’s lifespan had a larger quarterly decrease of 43%. Although both families decreased quarter over quarter, their lifespans were higher than our annual average.

Global DDoS IoT Threats Tracked by Country

The following DDoS-specific heatmaps represent the top 10 countries by C2s tracked and DDoS botnet hosts. The data is based on Black Lotus Labs' visibility and is broken down by threat type and suspected country of origin. The country of origin is determined by comparing the IP address of each host against a rich set of globally mapped IP addresses.

A note regarding heatmaps: just because the C2 infrastructure is located in a particular country, it doesn't mean that is its true origin. Cybercriminals often hide the source of their activity by leveraging infrastructure in other countries.

Top 10 Countries by C2

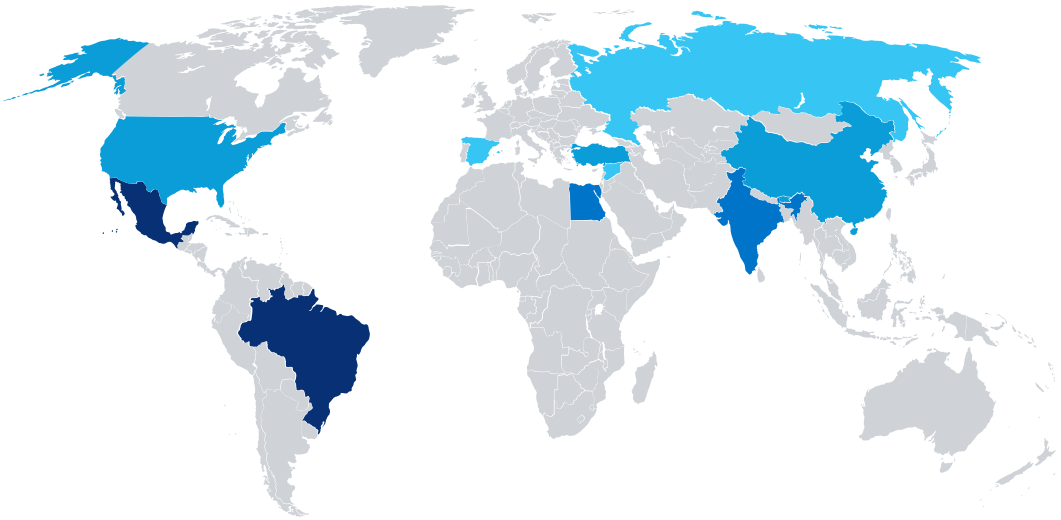


Country Name	C2s	Population*	Per Capita (100,000)
United States	554	331,002,651	0.17
The Netherlands	266	17,134,872	1.55
Canada	197	37,742,154	0.52
Germany	187	83,783,942	0.22
Spain	94	46,754,778	0.20
United Kingdom	79	67,886,011	0.12
France	36	65,273,511	0.06
Russia	29	145,934,462	0.02
Singapore	26	5,850,342	0.45
Vietnam	19	97,338,579	0.02

Lumen tracked 1,724 C2s globally in Q4; the heatmap above represents the countries with the most C2s. The United States had the most C2s and accounted for 32% of the total C2s tracked. Canada, The Netherlands, and Germany also had significant increases from previous

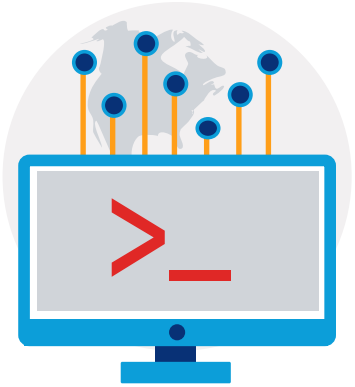
quarters. China, which had our number one spot last quarter, dropped off our top 10 list completely, along with South Korea and Taiwan. New entrants to the list are: UK (5% of total), France (2% of the total) and Singapore (2% of total).

Top 10 Countries by DDoS Botnet Hosts



Country Name	Bots	Population*	Per Capita (100,000)
Mexico	45,719	128,932,753	35.46
Brazil	41,616	212,559,417	19.58
India	25,304	1,380,004,385	1.83
Egypt	23,631	102,334,404	23.09
United States	14,359	331,002,651	4.34
China	10,658	1,439,323,776	0.74
Turkey	10,405	84,339,067	12.34
Spain	9,857	46,754,778	21.08
Russia	8,021	145,934,462	5.50
Syria	6,608	17,500,658	37.76

Black Lotus Labs observed a 17% increase in global DDoS botnet hosts quarter over quarter, with more than 250,000 — the highest we've seen all year. Our top country on the list, Mexico, had an increase of 7% and



went from the number two spot to the number one spot. Brazil moved down to our number two spot with a slight decrease of 7%. India experienced the biggest increase of 58% from Q3, going from around 15.9K botnet hosts to 25.3K hosts. China and Syria were new additions to the list, while Argentina and Lebanon fell off our top 10 list.

Takeaway #1

Why should I care about global data?

If you're a company in the United States, what does it matter if Mexico has the most botnet hosts? With Gafgyt and Mirai being so widely spread, there's always a chance you could become a victim, or your infrastructure could be used to target other organizations. If your network doesn't have the proper protection in place, you could be unwittingly participating in attacks against others. Being part of a botnet infrastructure can actually have negative impacts on your own operations, such as increased bandwidth costs and performance issues of your applications. And once a hacker has access to your systems, you're open to a myriad of attacks, from data theft to crypto mining or ransomware.

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

After a busy Q3, there was a slowdown in Q4

Looking at 2021, our busiest quarter was Q3 with more than 7,100 attacks mitigated. And July, in particular, saw the largest number of attacks in terms of frequency, size and duration. In Q4 we saw our lowest number of attacks per quarter at 3,718, which is a 48% quarterly decrease. However, there was almost no decline in the number of sites attacked (only a 3% decrease), which means that even though there were fewer attacks in the quarter, bad actors are spreading out the attacks to many more sites. A possible reason for the decrease could be seasonality. DDoS attacks ebb and flow like many other trends and in 2022 we expect to see activity continue to rise.

Attack Size and Duration

Largest Attack Scrubbed

	Dropped Bits/s	Dropped Pkts/s
Q4	499 Gbps	60 Mpps
Q3	612 Gbps	252 Mpps
QoQ Change	↓27%	↓76%

LUMEN® TECHNOLOGIES

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 by bits per second.
2. **Packet Rate Attacks:** These attacks consume resources on network elements such as routers and other appliances. These are typically larger than bandwidth attacks and measured in packets per second.

Bandwidth Attacks

In Q4, there was a 27% decrease in bandwidth attacks over Q3.

The average size of nearly 500 Gbps, however, was above our 2021 average of 450 Gbps.

The average attack size increased from 1 Gbps in Q3 to 2 Gbps in Q4.

Packet Rate Attacks

In Q4, the largest attack decreased by 76% from 252 Mpps to 60 Mpps.

Our average attack size in Q4 was 515 Kpps — a 68% increase over the previous quarter.

Takeaway #2

Why does attack size matter?

You don't need to be hit with the largest attack in history to see your business operations disrupted. We see a lot of organizations that don't have DDoS protection taken offline by sizes as small as 1 Gbps. Having DDoS protection in place will help ensure that web-facing assets continue to work even if you're under an active attack.

LUMEN® TECHNOLOGIES

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

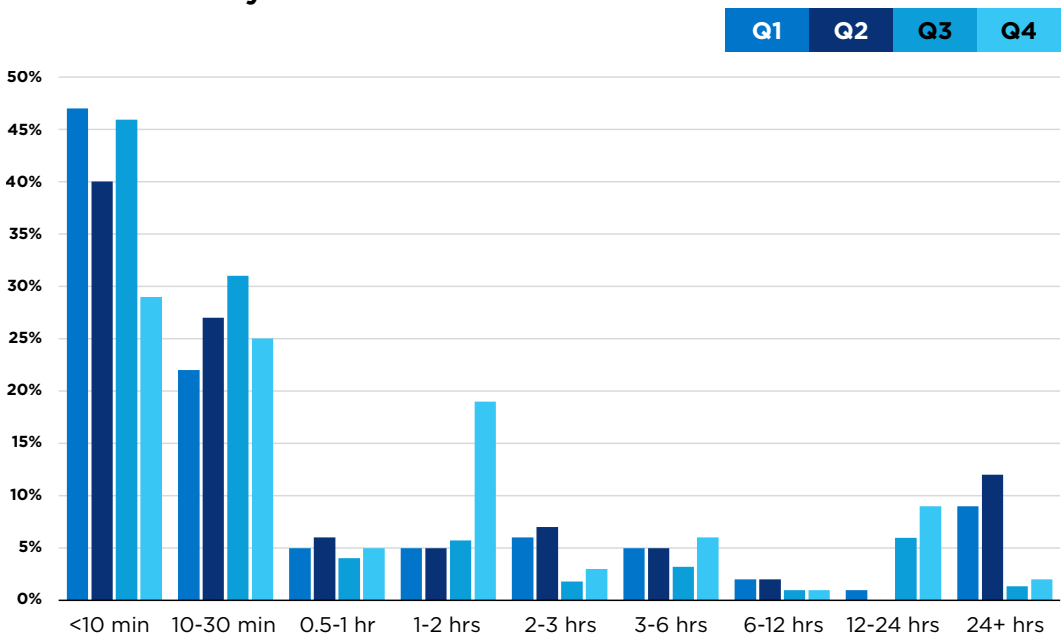
	Q4	QoQ Change
Median attack duration	30m	▲184%
Average attack duration	4h 23m 50s	▲75%
Longest attack duration	5 days	▼64%

When looking at how long attacks are lasting, we saw our average and median attack period durations increase by 184% and 75% respectively. Our median attack period duration was the longest we've experienced all year and had the largest jump from Q3 to Q4, going from just under 11 minutes to 30 minutes.

LUMEN® TECHNOLOGIES

The longest attack Lumen mitigated in Q4 was five days — a significant decrease from previous quarters. This doesn't mean that we can all breathe a sigh of relief. This decrease can be attributed to seasonality where DDoS actors weren't as active. We expect that longer and more sophisticated attacks are on the horizon.

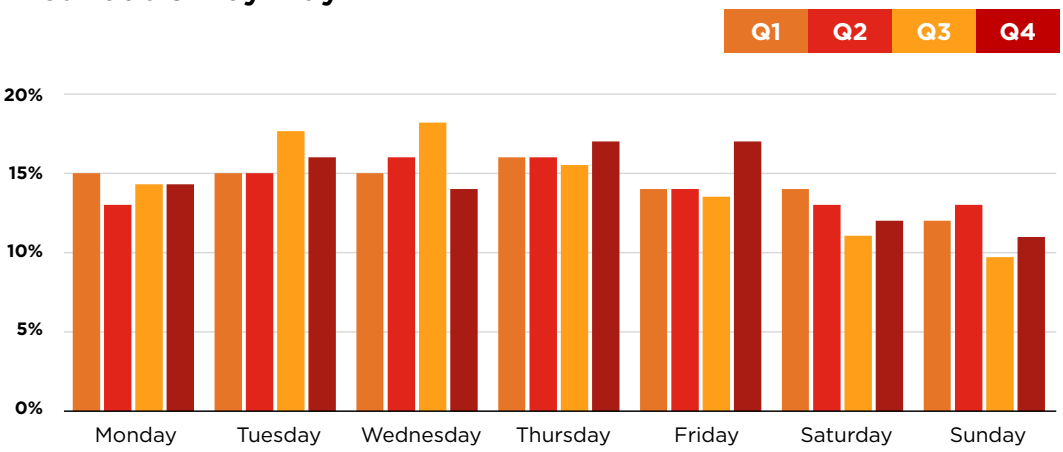
Distribution by Duration



As with the rest of 2021, in Q4, under 10 minutes is still the most prevalent duration, accounting for 29% of mitigated attacks. However, in Q4, for the first time in 2021, we observed a huge jump in attack durations lasting one to two hours. Typically, the percentage of attacks under 1-2 hours was around 5.5%, and in Q4 it jumped up to 19% of total attacks.

There were upticks in attack periods lasting 12-24 hours, and those lasting more than 24 hours (52% and 73% respectively). Earlier in the year, attackers had a much longer attack period with 9-12% of attacks lasting more than 24 hours; however, this is the first time we're seeing a heavier reliance on 12-24 hour attack period durations.

Distribution by Day



Attacks by day of the week were mostly in line with what we observed in the first three quarters. In Q3, Tuesdays were more active but in Q4 more activity happened on Fridays. Saturday and Sunday continue to remain the least active days.

The day with the most attacks we saw in Q4 occurred on December 16th, when Lumen mitigated 83 attacks, followed by November 18th, when we mitigated 79 attacks.

Takeaway #3

Can you afford to be down, even for just 30 minutes?

Attackers are looking to disrupt your operations. Can you afford for your web operations to be down for even just half an hour? Will your customers come to your app or site, see it's down and go elsewhere? Will people hear about the attack on your organization in the news and not trust you to protect sensitive data like payment information? Will you be fined by any compliance organizations? The cost of an attack is not just the downtime you suffer but can have long-reaching ramifications for your bottom line. In recent years, the average cost of a DDoS attack can be in the hundreds of thousands of dollars.

Attack Mitigation Types

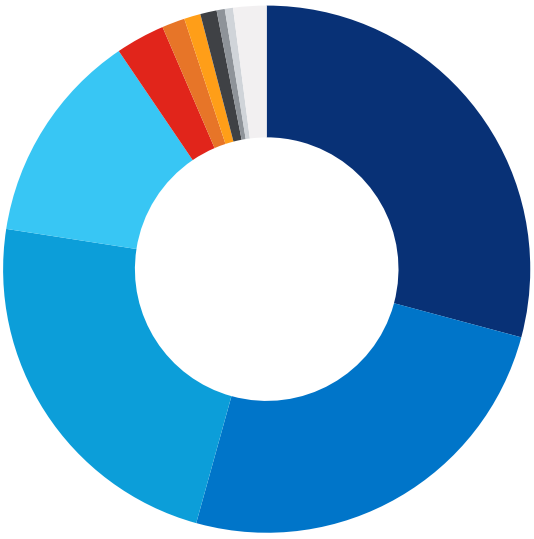
Multi/Single-Vector Attacks

	Q4	Q3	QoQ Change
Single-vector	65%	56%	▲16%
Multi-vector	35%	44%	▼20%

In Q4, we mainly saw single-vector attacks, which had a 16% quarterly increase, jumping from 56% to 65% of all attacks. This was the highest percentage of single-vector attacks all year.

Single-Vector Mitigations

Single-Vector Mitigation Type Breakdown



		QoQ
UDP	29%	▲60%
Invalid Packets	25%	▲89%
Static Filtering	23%	▲14%
TCP SYN	13%	▼48%
Other Volumetric	3%	▲6%
DNS Amplification	1.40%	▼87%
IP Fragmentation	1.00%	▼81%
HTTP	1.00%	▲67%
TCP RST	0.50%	▲45%
SIP	0.50%	▲54%
Other	2.03%	▲20%

When looking at the breakdown of single-vector mitigation types, UDP-based amplification skyrocketed to the top, accounting for 29% of all attacks and representing a 60% quarter-over-quarter increase. While UDP-based attacks are prevalent, they don't typically represent our most common type of mitigation. These attacks aim to consume

available bandwidth and have proven to be quite powerful with the ability to wield attacks multiple times the size of the initial bytes sent. If you're looking to learn more about UDP-based attacks read the Black Lotus Labs blog: Tracking UDP Reflectors for a Safer Internet.

Invalid packets were our second highest mitigation type, accounting for 25% of activity and an 89% increase from Q3. Invalid packet data includes traffic with malformed data fields, as well as incomplete fragments, duplicate, or too large packets. While they may be the result of network-related issues or faulty network sequencing, packet fragments are also a common characteristic of UDP amplification DDoS attacks.

Static filtering remains high among our single-vector mitigations at 23%, which is a 14% quarterly increase, and is in line with what we observed throughout 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	12%	N.A.
Invalid Packets, UDP	6%	▼6%
UDP, Static Filtering	5%	N.A.
Other Volumetric, UDP	4%	▲183%
Other Volumetric, UDP, Static Filtering	4%	▲123%
TCP SYN, Static Filtering	4%	N.A.
Invalid Packets, Static Filtering	3%	▲50%
Invalid Packets, UDP, Static Filtering	2%	N.A.
DNS Amplification, IP Fragmentation, Invalid Packets, UDP	2%	N.A.
TCP SYN, UDP	2%	N.A.

In Q4, DNS combined with TCP SYN accounted for the most activity when it came to multi-vector mitigations (12%).

We observed some new combinations this quarter. Most included UDP amplification, which mimics what we reported out for single-vector mitigations.

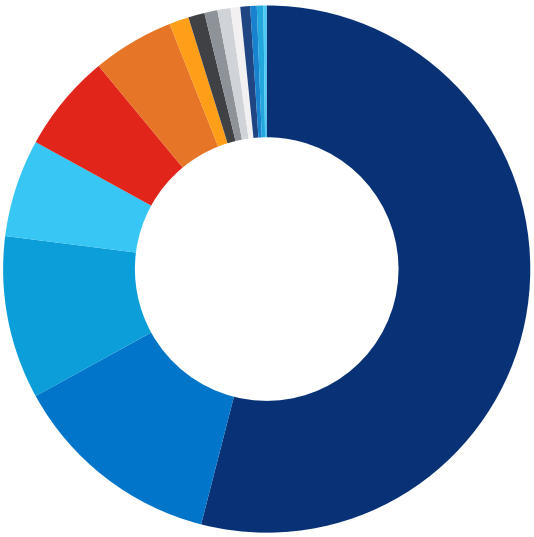
Takeaway #4

Cybersecurity is an arms race.

Do you know if you're protected against the latest threats? Cybercriminals can change attack parameters and vectors in response to new defenses they encounter. They have the financial motivation to continue to modify their attacks until they break down barriers. This can lead to an ongoing race between defense and offense to keep up with each other. Our Black Lotus Labs team works everyday to defend the global internet community and their threat intelligence is fed into four DDoS Mitigation solutions and other managed security solutions. Lumen helps protect against daily attacks on your critical resources with automated response policies.

Read data sheet

Largest 500 Attacks by Industry



Telecomm	54%
Gaming	13%
Software & Technology	10%
Hosting	6%
Government	6%
Finance	5%
Media & Entertainment	1.2%
Retail & Distribution	1.0%
Manufacturing	0.8%
Business Services	0.8%
Utilities	0.8%
Education	0.6%
Banking	0.4%
Other	0.4%
Healthcare	0.2%

Of the 500 largest attacks, 80% targeted these top five verticals (in order):

1. Telecommunications
2. Software and Technology
3. Retail and Distribution
4. Government
5. Gaming

We had some new entries to our top vertical list including Manufacturing and Healthcare. The gaming industry had the largest leap, doubling attacks that we saw throughout the rest of 2021. This could be because gaming companies prepare their 2022 releases in the latter half of 2021, so they become higher value targets during that timeframe. Below you can find more details on our top targeted industries.

Telecommunications

- **54%** of the largest 500 attacks
- **812** total attacks against vertical
- Largest bandwidth attack: **317 Gbps**
- Longest attack period duration: **4 days**
- **57%** multi-vector attacks
- Largest packet-based attack: **60 Mpps**

Gaming

- **13%** of the largest 500 attacks
- **129** total attacks against vertical
- Largest bandwidth attack: **59 Gbps**
- Longest attack period duration: **5 days**
- **80%** multi-vector attacks
- Largest packet-based attack: **5 Mpps**

Software and Technology

- **10%** of the largest 500 attacks
- **513** total attacks against vertical
- Largest bandwidth attack: **499 Gbps**
- Longest attack period duration: **3 days**
- **75%** single-vector attacks
- Largest packet-based attack: **71 Kpps**

LUMEN® TECHNOLOGIES

Hosting

- **6%** of the largest 500 attacks
- **106** total attacks against vertical
- Largest bandwidth attack: **408 Gbps**
- Longest attack period duration: **5 days**
- **61%** single-vector attacks
- Largest packet-based attack: **487 Kpps**

Government

- **6%** of the largest 500 attacks
- **754** total attacks against vertical
- Largest bandwidth attack: **26 Gbps**
- Longest attack period duration: **2 days**
- **57%** single-vector attacks
- Largest packet-based attack: **8 Kpps**

Takeaway #5

Am I safe if my industry isn't on the list above?

The list above includes the largest attacks we experienced, but nearly every vertical and every type of company can be and is attacked. If you have any sort of data that someone would want, your organization can be a target. If you want to learn more about attack trends in your vertical, please contact a Lumen sales representative to discuss.

Contact us

LUMEN® TECHNOLOGIES

Key Takeaways

The biggest thing that 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. Any time data moves there will be a vulnerability, but knowing the trends and what is going on in the cybersecurity space can help you identify vulnerabilities.

When it comes to DDoS attacks, a few things for you to keep in mind:

1. **No one is immune:** If you have valuable internet facing assets — bad actors will target your organization.
2. **No one can afford to be a victim:** With everyone being a potential target, one of those victims shouldn't be your bottom line. Costs of an attack include lost revenue, potential fines, damage to your reputation, and possibly the ransom to stop the attack.
3. **No one can do this by themselves:** With DDoS trends continually evolving, in-house security teams can't keep up or mitigate by themselves. The right partner can help bolster your existing security strategy.

Unsure if you're under a DDoS attack? Read our blog to recognize the signs: How to Tell If Your Business is Suffering From a DDoS Attack

If you don't have a DDoS mitigation partner or you're looking for a new one, here are some criteria to look for:

- Scale and capacity to absorb large attacks on the backbone as the first layer of defense.
- A global footprint for reduced latency when rerouting for scrubbing.
- Flexibility and advanced features to protect modern digital experiences.
- Visibility into the global threat landscape to bolster defenses.
- Automation based on threat intelligence to block DDoS bot traffic before it impacts the network.
- Hybrid support models to protect today's digital environments. From the remote employee to offices, and from the data center to the cloud.

How Lumen can help you today

With one of the largest DDoS Mitigation deployments in the industry, 85+ Tbps of global backbone FlowSpec capacity, next-gen intelligent scrubbing, and Black Lotus Labs-derived countermeasures, Lumen owns DDoS mitigation at scale. Lumen DDoS mitigation service delivers On-Demand and Always-On mitigation options with advanced features like intelligent scrubbing to help reduce latency and improve performance, and a flat monthly service rate regardless of size, length, or frequency of attacks.

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

Learn more about Lumen DDoS Mitigation

If you're interested, read our Q3 Quarterly DDoS Report

LUMEN® TECHNOLOGIES

Methodology

Data in this report is from the timeframe of October 1, 2021, through December 31, 2021.

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.

Endnotes

* Source: Worldometer (www.worldometers.info)

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

LUMEN® TECHNOLOGIES