REPORT

Lumen Quarterly DDoS Report

Q3 2021

LUMEN® TECHNOLOGIES

Introduction

Is anyone else tired? When looking at the sheer scale of the cybersecurity landscape it can feel like a never-ending stream of changes. Much like Sisyphus pushing the boulder up the mountain, just when you feel like you have a grasp of what's going on, a new attack happens and you're back at the bottom of the hill. But, in our humble opinion, security is the most vital part of working in the networking and IT space. This report is put together by Lumen employees who are passionate about cybersecurity, and about protecting organizations and creating a safer internet. And it starts with an unrelenting focus on attack types and methods.

Today, you'll find three major trends affecting organizations of all shapes and sizes:

1. Larger and more pervasive DDoS attacks.
2. IoT vulnerabilities and command and controls (C2s) extending their reach.
3. Cybercriminals of varying expertise are launching attacks with more frequency, larger volumes and increased complexity.

Although it may seem it's becoming harder and harder to push the boulder up the mountain, this report will help you understand spoof reflection attacks, why global IoT botnet trends matter, how attacks are changing quarter over quarter and who is being targeted — so you can bolster your defenses.

In our Lumen Quarterly DDoS Report for Q3 2021, we examined intelligence from Black Lotus Labs® and data from the Lumen® DDoS Mitigation platform to develop our findings, which both reinforce and expand on these broader trends.

Table of Contents

LUMEN® TECHNOLOGIES

Key Findings for Q3 2021

IoT DDoS Botnets

- There was a 26% quarterly decrease in unique C2s tracked for pervasive DDoS botnets Gafgyt and Mirai.
- The average lifespan of a Gafgyt C2 was 38 days, while Mirai's C2 average lifespan was 21 days.
- Lumen tracked a little over 2,100 C2s globally. The countries with the most C2s were (in order): China, United States and, tied for third, Taiwan and the Netherlands.
- We observed a 45% quarterly increase in the number of DDoS botnet hosts globally. The countries with the most DDoS botnets were (in order): Brazil, Mexico and Egypt.

DDoS Attack Trends

- The number of attacks we mitigated increased by 35% compared to Q2.
- The largest bandwidth attack we scrubbed in Q3 was 612 Gbps, which is a 49% increase quarter over quarter.
- The largest packet rate-based attack we scrubbed in Q3 was 252 Mpps, which is a 91% increase quarter over quarter.
- The longest DDoS attack period we mitigated for an individual customer lasted 14 days.
- 46% of attack-period durations were under 10 minutes, when looking at our On-Demand DDoS customers.
- Multi-vector mitigations represented 44% of all DDoS mitigations, with the most common combination being: DNS amplification, TCP RST, TCP SYN-ACK amplification and UDP amplification.
- TCP SYN was the most common single-vector mitigation type, accounting for 25% of DDoS mitigations.
- The top three targeted verticals in the 500 largest attacks in Q3 were: Telecom, Software and Technology, and Retail.

Spoofed Reflection Attacks: Crank Phone Calls with Immense Impacts

What are they?

Before we get into the nitty gritty of what we're seeing, let's start off with a definition of what an amplification or spoofed reflection attack is. A spoofed reflection DDoS attack is one where an actor pretends to be another entity and initiates a slew of communications to elicit a flood of traffic back to the unsuspecting victim.

Let's say an attacker wants to target Company X with a reflection DDoS attack. The attacker sends a request to a network server asking for information, providing Company X's IP address as the sender instead of its own. The server, thinking it's being helpful, sends the information back to Company X. Now that doesn't sound so bad. But the attacker wants to disrupt operations. Using mainly UDP servers that are misconfigured as open reflectors, the attacker can make the response back to Company X exponentially larger than the original request. On top of that the attacker, still using the spoofed IP address, commands all hosts in their botnet to send the same request to multiple servers using the same source IP, leading Company X to be overwhelmed very quickly.

You can imagine it's like someone pretending to be you calling a restaurant and ordering a pizza. In addition to that pizza, they say, "send me another pizza every 15 minutes." On top of that, they get all of their friends to call the restaurant with the same request. You have no clue where the requests came from and you're overwhelmed by all the pizzas arriving at your house. That's quite a mess to clean up!

How can you stop spoofed reflection attacks?

The problem is, spoofed reflection attacks are very difficult to mitigate yourself, and options are usually limited for targets. Cybercriminals aren't just looking to cause chaos; crime pays. Given the difficulty of tracing spoofed reflection attacks, they are a hot commodity on the dark web. A hacker can rent their infrastructure, attack code, etc., to anyone who's interested.

So, how do you clean the internet from bad actors when there's such a large pool of attackers that are well-hidden? Lumen is partnering with industry trust groups to help track these attacks back to their original sources. Due to our network size and threat hunting capabilities, we analyze NetFlow and use other techniques to find the ingress of the traffic, whether that is a peer interconnected with Lumen or a customer. In addition to industry peer partnerships, when we identify a customer that has open reflectors being abused visibily, we recommend they close the service or make configuration changes to mitigate potential abuse.

We've traced the untraceable, now what? That's a question that providers like Lumen have struggled with. There is no single solution to detect or filter these attacks, but we use options such as access control lists, firewall filters, BGP FlowSpec and unicast reverse-path-forwarding. Ultimately, the source of the spoofed traffic — other network providers — are responsible for cleaning up their own activity.

All is fair in love, war and cybersecurity.

When an organization is told that it's the main source of an attack, you would expect action. But we've found that's not always the case. As one example, in Q3 an industry trust group called out a major attack that was impacting a large company. The Lumen Security Operations Center (SOC) used data from Black Lotus Labs to find the top ingress network, a large Russian ISP. When the attack was brought to their attention, they said there was no evidence of the attack. After much back and forth, the ISP continued to drag its feet. The suspicious activity led us to believe they were potentially doing this intentionally to protect revenue from a black hat client, or at the very least, they were complacent.

The ISP customer was sent an Acceptable Use Policy (AUP) violation; however, no action was taken, and the attacks continued. Lumen continued to try to work with the ISP, but ultimately Lumen had to implement large access control lists to filter the bad traffic.

Despite this, the attacks continued, albeit smaller. Finally, we got to the breaking point. In accordance with the AUP, we had the right to disconnect them from the network, unless action was taken, so Lumen ultimately came in with a more prohibitive access control list to mitigate the situation.

Takeaway #1

So what do I do if I think my organization is under a spoofed reflection attack?

Given the complex nature and the large scale of these attacks, you're going to have to work with an established DDoS mitigation provider. This isn't just about protecting your organization from the act itself, but also tracking down complicit and responsible parties. It is every ISP's responsibility to sweep their network for unsecured reflection servers to ensure they are patched against being utilized for DDoS. Limiting access on these servers to only trusted communications is also a solid security best practice. Lastly, partnering with your upstream ISP if they notify you of a potential AUP violation will help clean up threats that may have been reported by victims of malicious activity. We are all in this together!

IoT DDoS Botnets

Family	Unique C2s tracked	Unique attack victims per family	Average lifespan of a C2 (in Days)
Gafgyt	349 ▼31% QoQ	Data inconclusive	38 ▲19% QoQ
Mirai	284 ▼19% QoQ	22,308 ▲43% QoQ	21 ▼25% 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. Q3 data was on par with what we have found in previous quarters. Though, due to the shifting nature of botnet activity, we expect to see the figures ebb and flow. Overall, there was a

26% quarter-over-quarter decrease in the unique C2s Lumen tracked, with Gafgyt accounting for most of the decrease, dropping 31% since Q2.

We define “victims” as the number of unique IPs against which we observed the C2s launching DDoS attacks. While we continue to track the Gafgyt family, this quarter our victim data was inconclusive. However, Mirai victims increased 43% from what we reported in Q2 and are now roughly equivalent to our Q1 findings.

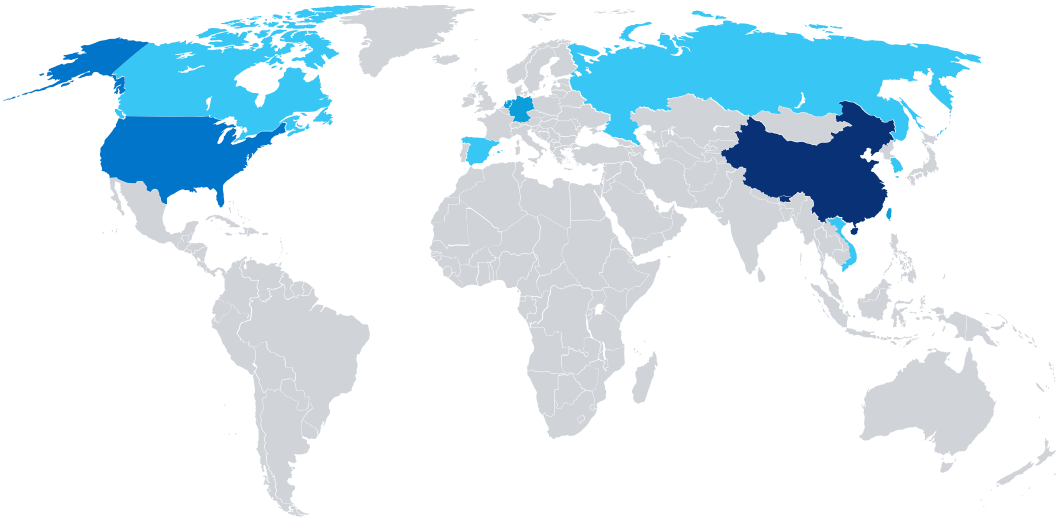
Bad actors’ goal is to cultivate reliable infrastructure they can use for their own attacks or to rent as a service to other actors for temporary use. Again, we expect some ebb and flow in these figures as botnets evolve. This quarter, the average lifespans for Gafgyt and Mirai are similar to what we saw in Q2. Gagyt’s average lifespan increased by 19% and Mirai’s decreased by 25% in Q3.

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 are based on Black Lotus Labs visibility and is broken down by threat type and suspected country of origin. Country of origin is determined by comparing the IP address of each host against a rich set of globally mapped IP addresses.

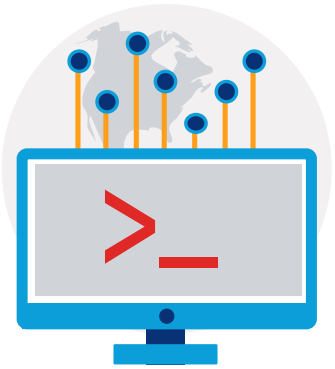
A note regarding the heatmaps: Just because the C2 infrastructure is located in a particular country doesn’t mean that is the infrastructure’s true origin. Cybercriminals often hide the source of their activity by leveraging infrastructure in other countries.

Top 10 Countries by C2



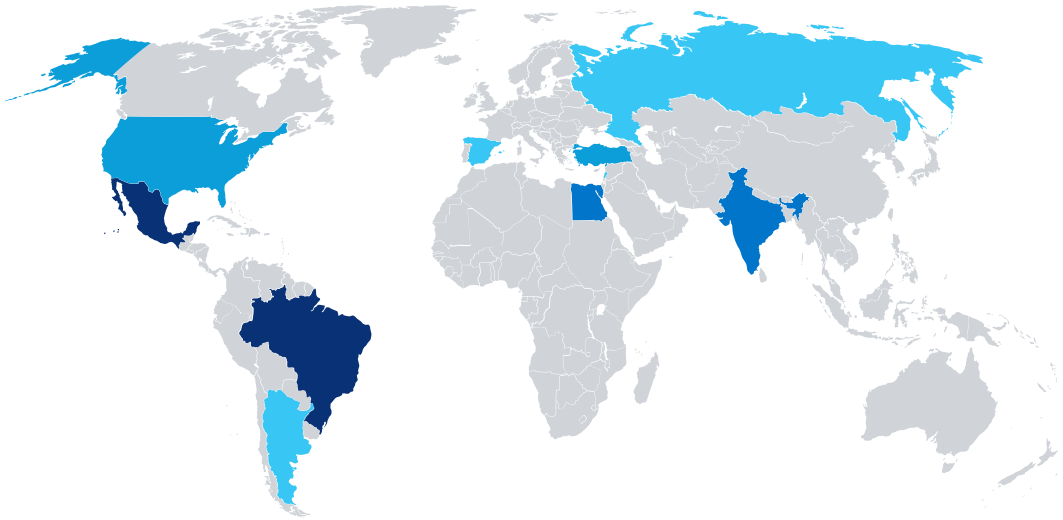
Country Name	C2s	Population*	Per Capita (100,000)
China	653	1,439,323,776	0.05
United States	381	331,002,651	0.12
Taiwan	128	23,816,775	0.54
The Netherlands	128	17,134,872	0.75
Germany	115	83,783,942	0.14
South Korea	88	51,269,185	0.17
Vietnam	74	97,338,579	0.08
Canada	56	37,742,154	0.15
Russia	51	145,934,462	0.03
Spain	39	46,754,778	0.08

Lumen tracked 2,102 C2s globally; the heatmap above represents the countries with the most C2s. The APAC region saw an increase in C2s this quarter, accounting for four of the top 10 spots, tied with Europe. The country with the most DDoS C2s was China, with 653 or 31% of the total C2s Black Lotus Labs tracked in Q3. The United States fell to the number two spot after being first in Q2, and Taiwan, new to the list, tied for third with the Netherlands. Other new countries that were added to the top 10 list include South Korea and Vietnam, while United Kingdom, Italy, Iran and France all fell below the top 10.



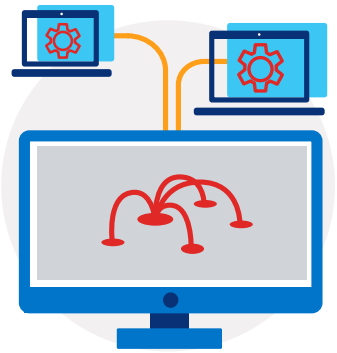
LUMEN® TECHNOLOGIES

Top 10 Countries by DDoS Botnet Hosts



Country Name	Bots	Population*	Per Capita (100,000)
Brazil	44,837	212,559,417	21.09
Mexico	42,736	128,932,753	33.15
Egypt	19,546	102,334,404	19.10
India	15,975	1,380,004,385	1.16
United States	10,266	331,002,651	3.10
Turkey	10,171	84,339,067	12.06
Russia	8,854	145,934,462	6.07
Spain	8,044	46,754,778	17.20
Argentina	5,976	45,195,774	13.22
Lebanon	5,467	6,825,445	80.10

Black Lotus Labs observed a 45% increase in global DDoS botnet hosts quarter-over-quarter, with over 217,000 — the highest we've seen all year. Our top three countries saw big increases this quarter: Brazil: 35%, Mexico: 78% and Egypt: 129%. Lebanon, a new entrant to the top 10 list, has the most bots per capita — coming in around 80, with Mexico the second highest at 33. Spain was also a new addition to the list, while China and Iraq fell below the top 10 line.



Takeaway #2

What does this global data mean?

You may be asking yourself: "Why does it matter what's happening in Brazil if I only conduct business in the United States?" These two longstanding malware families have become so widespread that there's a high risk of being targeted. And there's also more than one way to be impacted. If your network doesn't have the proper protections in place, you could be unwittingly participating in attacks against other organizations. Simply being part of a botnet can lead to increased bandwidth costs and performance issues for your online tools and applications. And once a hacker has access to your system, you're now open to a myriad of attacks, from information stealing to crypto mining to 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 discoveries and adversary takedowns from Black Lotus Labs, read their blogs.

Read now

LUMEN® TECHNOLOGIES

DDoS Attacks by the Numbers

Takeaway #3

It's not if, it's when...

Lumen mitigated a total of 7,185 DDoS attacks in Q3. This is a 35% increase from second quarter and the highest we've experienced this year. We are protecting against an average of 80 attacks a day, which has been steadily increasing from 67 per day in Q1. Bad actors are getting bolder and more sophisticated, and they are looking to cause more disruption than ever. We have observed increasing levels of complexity in the number of attack methods used against our customers.

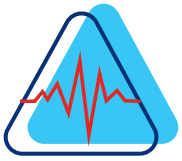
The best defense is to have a strategy. If you're looking for a DDoS mitigation service that can go toe-to-toe with the evolving threat landscape, explore our DDoS mitigations services.

Learn more

Lumen may mitigate large-scale DDoS attacks across its global backbone before traffic ever reaches a scrubbing center. Attack sizes in this report convey the largest attacks scrubbed by Lumen global DDoS scrubbing infrastructure, rather than the largest attacks observed transiting or being scrubbed by the Lumen network.

Attack Size and Duration

Largest Attack Scrubbed



	Dropped Bits/s	Dropped Pkts/s
Q3	612 Gbps	252 Mpps
Q2	419 Gbps	132 Mpps
QoQ Change	▲46%	▲91%

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.

Lumen observed significant increases in the largest attacks that we scrubbed. There have been nearly linear increases throughout the year in the largest bandwidth attacks. In Q3, there was a 46% increase in the largest attack, going from 419 Gbps to 612 Gbps. While we're seeing the largest packet rate attacks increase exponentially in 2021, jumping from 132 Mpps in Q2 to 252 Mpps this quarter.

But you don't need to be hit with the largest attack to see your operations disrupted. The average attack size we saw (1 Gbps for bandwidth, 307 Kpps for packet rate) could easily take unprotected organizations offline.

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.

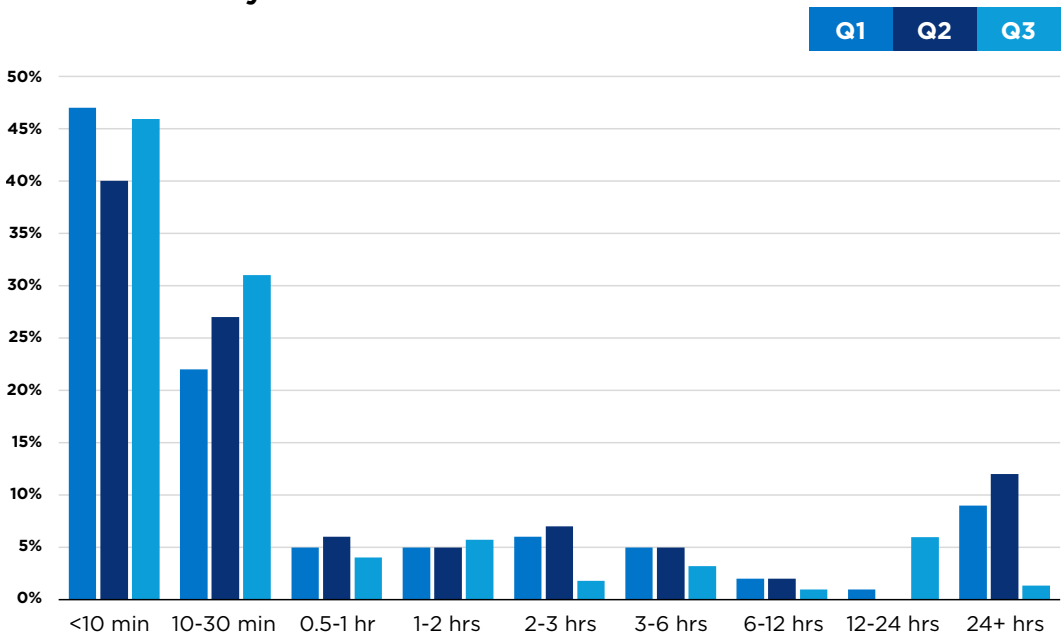
The data below only portrays trends for On-Demand customers, which accounts for 84% of attacks Lumen mitigated in Q3. Learn more about the differences between On-Demand and Always-On mitigation.

Watch video

	Q3	QoQ Change
Median attack duration	10m 56s	↓30%
Average attack duration	2h 42m 22s	↓41%
Longest attack duration	14 days	↑40%

Attack duration data suggests that the most frequent attacks are short in duration (<10 minutes). We did see a slight decrease in median attack duration from 15 minutes in Q2 to just under 11 minutes in Q3. One of the possible causes of this downward trend could be the reliance on ransom DDoS, where bad actors deploy a small attack to prove they're serious in their intent to launch bigger attacks. Our longest attack-period duration increased back up to 14 days — the same level we reported in Q1.

Distribution by Duration

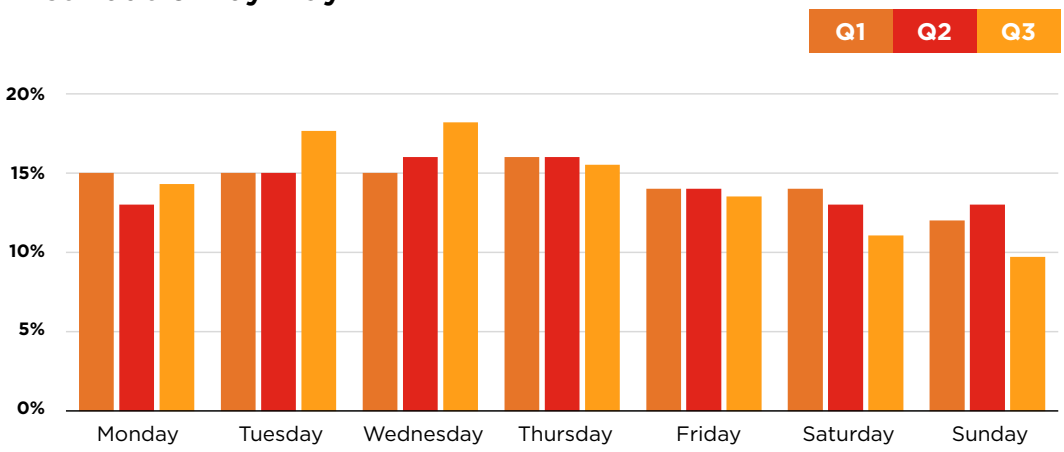


LUMEN® TECHNOLOGIES

When looking at the attack-period duration, 46% of attacks were under 10 minutes, which matches our findings from Q1. We also saw attacks in the 10-30 minute range at their highest this year, accounting for 31% of activity. Where we saw the biggest drop-off was in the over 24-hour attacks, going from 12% of attacks in Q2 to around 1% in Q3. A possible explanation is the typical shift in tactics that occur throughout the year, with actors currently focusing on more frequent and quicker attacks.

When we compared attack duration to attack size, we observed that the longer attacks tend to be larger in scale as well. For example, the largest attack (612 Gbps at its peak) had an attack-period duration of 48 hours.

Distribution by Day



Attacks by day of the week were mostly in line with what we observed in the first two quarters of 2021, except for Tuesday, Wednesday and Sunday. Skewed by attacks we saw in the retail space early in the quarter, Tuesday and Wednesday each had 18% of attack activity. Meanwhile, Sunday decreased to the least likely day for an attack going from 13% to 10% of attacks occurring on that day.

The days with the most attacks we saw in Q3 were July 6, when Lumen mitigated 240 attacks, followed by July 7 with 206 attacks mitigated.

LUMEN® TECHNOLOGIES

Takeaway #4

10 minutes doesn't seem bad until you look at the dollar signs

Looking at this data you might think, "Well I won't be faced with the longest attack — what are the chances of that?" And while that's true, you might not have to withstand the longest or largest attack, shorter attacks are just as effective at disrupting your organization. Let's say you have a customer who wants to access your app, and it's not available because you're unprotected and have an active DDoS attack. How long will that person try to access your application before giving up and going somewhere else?

Now let's say you're down for over two hours (our average). How much revenue have you lost? The average cost of IT downtime is in the hundreds of thousands of dollars. This doesn't even consider that customers may choose to go somewhere else to obtain the products or services you offer, or the brand reputation losses that will occur. Having solid DDoS protection in place will help prevent loss of revenue and productivity.

Attack Mitigation Types

Multi/Single-Vector Attacks

	Q3	Q2	QoQ Change
Single-vector	56%	62%	▼9%
Multi-vector	44%	38%	▲40%

With the overall number of attacks increasing this quarter, we saw both multi-vector and single-vector attacks increase. However, multi-vector attacks had a surge this quarter, representing 44% of all attack

mitigations. This is the highest that we've seen to date in 2021, showing that bad actors are relying on more and more complex attack vectors when targeting organizations.

Single-Vector Mitigations

Single-Vector Mitigation Type Breakdown

		QoQ
TCP SYN	25%	▲66%
Static Filtering	21%	▼26%
UDP	18%	▼17%
Invalid packets	13%	▼21%
DNS	11%	▲34%
IP Fragmentation	5%	▲28%
Other volumetric	3%	▼37%
ICMP	2%	▲56
HTTP	1%	▼43
DNS Amplification	0.64%	N.A.
Other	1.69%	N.A.

As new methods of attack arise, we expect these results to fluctuate. But even as new attack vectors will come and go, the tried-and-true methods continue to be relied upon. For example, TCP SYN was the most common type of single-vector mitigation we saw in Q3, which accounted for 25% of activity. This was a 66% increase from Q2 findings. Countermeasures for static filtering and UDP amplification fell from the one and two spots down to two and three, respectively.

Static filtering countermeasures are typically done on items such as port and protocol. This countermeasure is also where our Black Lotus Labs threat feed mitigations are captured. It provides initial mitigation against attacks and was 21% of single-vector attacks in Q3.

UDP-based amplification attacks continue to be prevalent, sitting at our number three spot with 18% of activity. These attacks aim to abuse application layer protocols and have proven to be quite powerful with the ability to wield attacks multiple times the size of initial bytes sent. If you're looking to learn more about UDP-based attacks, read our blog: Tracking UDP Reflectors for a Safer Internet.

Multi-Vector Mitigations

Top Multi-Vector Mitigation Type Combinations

		QoQ
DNS Amplification, TCP RST, TCP SYN/ ACK Amplification, UDP	28%	N.A.
DNS, TCP SYN	12%	▲23%
DNS, TCP SYN, Static Filtering	4%	▲35%
DNS, Static Filtering	3%	▲14%
Static Filtering, UDP	3%	▼43%
TCP SYN, Static Filtering	3%	▼36%
UDP, Static Filtering	2%	▼62%
DNS Amplification, IP Fragmentation	2%	▼10%
Other volumetric, UDP	2%	N.A.

For the first time this year, bad actors leveraged a much larger variety of attack vectors when launching multi-vector attacks. In previous quarters, Lumen observed a maximum of three simultaneous attack vectors, and this quarter we saw four: 28% of multi-vector mitigation were a combination of DNS amplification, TCP RST, TCP SYN-ACK amplification and other UDP amplification.

The second most common combination was DNS and TCP SYN, which was 12% of the multi-vector mitigations, up from 10% in Q2.

Takeaway #5

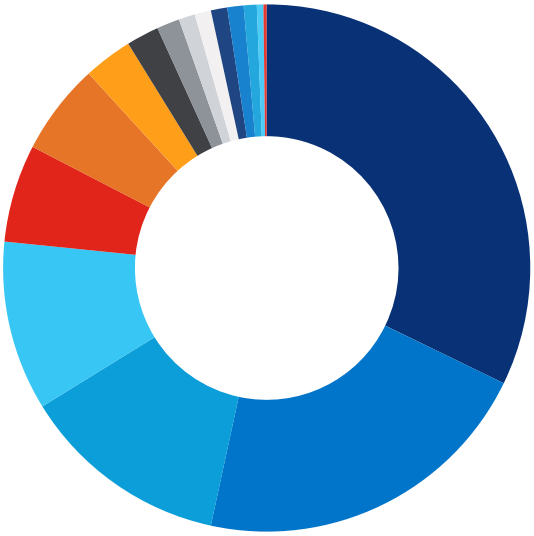
Don't DIY DDoS Protection

If you grade your cybersecurity practices, do you have an A+? Very few organizations do, and very few can afford to invest in large-scale mitigation infrastructure or hire the in-house talent needed to keep up with the barrage that the DDoS landscape presents. As more organizations seek to protect their infrastructure, bad actors are becoming craftier. They're going to come at you with everything they can to slip into your web-facing assets and applications. Cybercriminals can change attack parameters and vectors in response to defenses that they encounter when trying to launch an attack. They'll continue to modify the attack, so it becomes more difficult to mitigate against. Consider a DDoS mitigation solution that has automation built in its core functionality. Learn about Lumen Rapid Threat Defense.

View data sheet

LUMEN® TECHNOLOGIES

Largest 500 Attacks by Industry



Telecomm	34%
Software & Technology	21%
Retail & Distribution	12%
Government	7%
Gaming	6%
Hosting	8%
Media & Entertainment	4%
Finance	2%
Transport	2%
Banking	1%
Education	1%
Other	0.4%
Business Services	0.4%
Pharmaceutical	0.2%
Consulting	0.2%
Utilities	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 verticals list including: Retail and Distribution, Pharmaceutical, and Consulting. Retail and Distribution has the largest jump in Q3, representing none of our 500 largest attacks in Q2, to 12% in this quarter. Below you can find more details on our top targeted industries.

Telecommunications

34%
of the largest 500 attacks

956
total attacks against vertical

Largest bandwidth attack:
612 Gbps

Longest attack period duration:
6 days

52%
multi-vector attacks

Largest packet-based attack:
252 Mpps

LUMEN® TECHNOLOGIES

Software and Technology

- **21%** of the largest 500 attacks
- **515** total attacks against vertical
- Largest bandwidth attack: **405 Gbps**
- Longest attack period duration: **5 days**
- **60%** single-vector attacks
- Largest packet-based attack: **33 Mpps**

Retail and Distribution

- **12%** of the largest 500 attacks
- **425** total attacks against vertical
- Largest bandwidth attack: **116 Gbps**
- Longest attack period duration: **3 days**
- **60%** single-vector attacks
- Largest packet-based attack: **11 Mpps**

Government

- **7%** of the largest 500 attacks
- **2,565** total attacks against vertical
- Largest bandwidth attack: **44 Gbps**
- Longest attack period duration: **4 days**
- **62%** single-vector attacks
- Largest packet-based attack: **8 Mpps**

Gaming

- **6%** of the largest 500 attacks
- **215** total attacks against vertical
- Largest bandwidth attack: **6 Gbps**
- Longest attack period duration: **3 days**
- **53%** multi-vector attacks
- Largest packet-based attack: **886 Kpps**

LUMEN® TECHNOLOGIES

Takeaway #6

If I don't see my industry on the list, I won't be attacked, right?

The list above includes the largest attacks we experienced, but nearly every vertical and every type of company is attacked. A question to ask yourself: Do I have information someone would want? And the answer for every organization is yes. You have personal information on customers and employees. Any form of data can be valuable to hackers, and DDoS attacks are commonly used as a distraction for a larger data breach or a way to extort payment. If you want to learn more about attack trends in your vertical, please contact a Lumen sales representative to discuss.

Contact us

Key Takeaways

DDoS attacks are rampant today, and the frequency doesn't seem to be slowing down. If anything, it's evolving and changing so attacks are becoming more complex, larger and longer. Throughout the report, we've mentioned some takeaways for our readers:

1. Spoofed reflection attacks require the help of a DDoS mitigation provider because they can grow exponentially and require extreme mitigation tactics.
2. Global attack trends aren't "far off findings" that don't apply to businesses. In fact, you could easily be a target of C2s, or you could unwittingly be part of a botnet attacking other organizations.
3. With more and more attacks happening every day, it's no longer a matter of if you're going to be attacked but when. And it doesn't matter if you're not hit with the largest or longest attack; any attack can still disrupt operations.
4. Even 10 minutes of downtime can be more costly than you might think.
5. We saw some of the most complex attacks occurring in Q3; DIYing your DDoS strategy is a mistake.
6. Data is today's currency, and everyone is a target, no matter the industry.

The threat landscape can seem overwhelming. There's so much to watch out for and the stakes can be incredibly high. DDoS mitigation solutions can take some of the pressure off IT departments. When you look at the balance of DDoS mitigation costs versus the cost of attack in terms of revenue, productivity, reputation and customer experience, it's an easy choice.

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

- Scale and capacity to absorb large attacks on the backbone as a first layer of defense.
- A global footprint for reduced latency when rerouting for scrubbing.
- Flexibility and advanced features to protect modern digital experience.
- 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 remote employees, 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 Q2 Quarterly DDoS Report

LUMEN® TECHNOLOGIES

Methodology

Data in this report is from the timeframe of July 1, 2021, through September 30, 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