

REPORT

# Lumen Quarterly DDoS & Application Threat Report

Q1 2023

---

# Executive Summary

While this year presents exciting opportunities for growth and progress, it also brings new challenges for cybersecurity. Companies and other organizations are planning for growth — and so are cybercriminals. Make no mistake: they will continue to look for opportunities to exploit vulnerabilities in applications, APIs, and networks.

In this report, we provide up-to-date insights and analysis on the latest security trends and threats facing businesses and individuals alike. With a focus on DDoS, application, and API attacks we offer actionable intelligence to help you stay ahead of cybercriminals and protect your assets. We have expanded the purview of the report to analyze the application threat landscape in an effort to give our readers a more holistic view of attack trends.

As you plan your own strategies for the year ahead, we encourage you to use this report as a valuable resource to identify potential risks and prioritize areas for improvement. Our team of experts has carefully curated the most relevant information to help you navigate the ever-changing landscape of cybersecurity.

In our Lumen Quarterly DDoS and Application Threat Report for Q1 2023 you will learn about:

## DDoS

- An overview of the cybercriminal group: KillNet
- Attack sizes, lengths, and frequencies
- Attack vectors
- Targeted industries

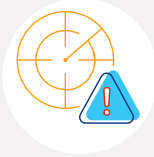
## Application Threats

- Blocked traffic
- Blocked traffic by industry
- Why suspicious traffic was blocked

Lumen examined data from the Lumen® DDoS Mitigation platform and our API and Application Protection partner, ThreatX, to develop this report. Both reinforced and expanded on broader trends.

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

1



**Sophisticated attack methods are on the rise:** Attackers continue to experiment with sophisticated attack types, new and old. Over Q1, there has been a significant increase in the use of DNS water torture attacks which uses a vector that cannot be outright blocked and require more sophisticated countermeasures to defend.

2



**A new year brings new multi-vector combinations:** Attackers are beginning to string many types of attack vectors together in attempt to disrupt businesses. With multi-vector combinations of five and six attack vectors, this is the most we have ever seen in the data.

3



**“Hit-and-run”-style attacks remain popular:** Short attacks lasting less than 10 minutes continue to increase in numbers, but we’re seeing the same victims targeted multiple times to cause long-term chaos.

4



**Beware of bots:** Applications are under immense pressure from swarms of malicious bots scouring the internet.

# Table of Contents

Cyber warfare within the Ukraine/Russia conflict .....	5
How many DDoS attacks were there? .....	7
How large are the DDoS attacks? .....	7
How long are DDoS attacks lasting? .....	8
What do DDoS attacks look like? .....	9
Who is being attacked? .....	12
What is the cost of a DDoS attack? .....	13
Application Protection .....	14
What application traffic is being blocked? .....	14
Blocked traffic by industry .....	15
Most blocked application suspicions .....	16
Final thoughts from Lumen .....	17

# Cyber warfare within the Ukraine/Russia conflict

## Where does this threat intelligence come from?

Our DDoS mitigation operations and Black Lotus Labs® teams work together to develop this report and provide insights for our readers.



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 help protect our customers and keep the internet clean. Black Lotus Labs uses threat hunting and analysis, along with machine learning and automated threat validation to identify and disrupt the work of malicious actors.

If you're interested in learning more about Black Lotus Labs' latest research, or to read about advanced actor and crimeware tracking, visit the blog archive.

[Read now](#)

Last year, the [Q1 2022 DDoS Report](#) discussed the conflict between Russia and Ukraine. A year later the conflict continues with no signs of slowing down. As the Ukrainian government and citizens struggle to cope with the escalating conflict and chaos, they also continue to face threats from pro-Russian cybercriminal entities such as KillNet.

## Who is KillNet?

KillNet is a pro-Russian cybercriminal organization that is actively involved in the ongoing conflict in Ukraine. Its mission is to add to the chaos by disrupting the networks of Ukrainian businesses, government agencies, and healthcare organizations. KillNet also launches DDoS attacks on NATO countries that support Ukraine; however, healthcare has been its primary focus lately.

For healthcare-targeted attacks, KillNet's main goal is to significantly damage critical healthcare infrastructure by overloading the targets' networks and hindering their ability to function. The U.S. Department of Health & Human Services Health Sector Cybersecurity Coordination Center ([HC3](#)) has been tracking KillNet since January 2022. HC3 states that, if successful, these attacks could "[prevent] patients or healthcare personnel from accessing critical healthcare assets such as electronic health records, software-based medical equipment, and websites necessary to coordinate critical tasks."

Looking back on 2022, KillNet made some remarkable threats against healthcare systems across the globe. In May, after a key member of the group was arrested in connection with attacks on Romanian government websites, KillNet [demanded](#) his release or threatened they would "target life-saving ventilators in British hospitals."

On a separate occasion, [HC3 notes](#) that the pro-Russian cybercriminals "threatened the U.S. Congress with the sale of the health and personal data of the American people because of the Ukraine policy of the U.S. Congress."

Although KillNet continues to publicly threaten healthcare systems, the cybersecurity industry seems to agree that their attacks have been relatively unsophisticated, resulting in more of an annoyance than a serious threat — so far.

The [Healthcare Innovation Group](#) notes that KillNet attempted a coordinated attack on 14 medical centers in the U.S. including Stanford Healthcare, Duke University Medical School and Cedars Sinai on Jan. 30, 2023. The attack had little to no impact on the targets, which could suggest the group's bark is bigger than its bite. This doesn't mean any organization can relax, however, which is why the Cybersecurity and Infrastructure State Agency ([CISA](#)) advised critical infrastructure organizations to take proactive measures to strengthen their security systems and defend against attacks from KillNet and other cybercriminals.

## KillNet misconceptions

The common misconceptions related to KillNet involve its motives, financial backing, and attack methods.

### Misconception #1: KillNet's purpose is to attack Ukraine on behalf of the Russian government.

**Reality:** While KillNet is believed to be sympathetic to the Russian government, there is no concrete evidence to suggest they are directly sponsored by the Kremlin. In addition, their attacks have not been solely targeted at Ukrainian entities. In fact, KillNet has been linked to attacks on several other countries including Romania, Moldova, Czechia, Italy, Lithuania, Norway, Latvia, the United States, Japan, Georgia and Germany.

Some of these countries' security entities were attacked, but the group has not limited itself to attacks on government. In 2022, KillNet is accused of attempting to launch a DDoS attack on the massive Eurovision song contest the night a Ukrainian artist performed, but the Italian government claims it thwarted the attack. (KillNet subsequently denied launching the attack only after it was unsuccessful, and the Ukrainian artist won the contest.)

### Misconception #2: KillNet's motivations are solely political.

**Reality:** As with other cybercriminal organizations, KillNet has financial motives, as evidenced by their use of [ransom DDoS attacks](#) and [brute-force dictionary attacks](#). In late October 2022, a cybersecurity channel by the name of PCrisk [tweeted](#) they have discovered the first sample of KillNet ransomware. For more information on how KillNet uses ransomware attacks, view [this article](#) from Firewall Daily.

By understanding these misconceptions, individuals and organizations can better prepare themselves to defend against KillNet's malicious activities.

## Killing KillNet

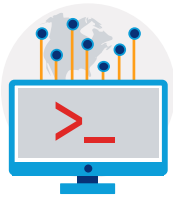
There are a few theories about why KillNet is targeting healthcare so aggressively. Perhaps these initial threats and attacks were scare tactics to gain attention. Or maybe KillNet is probing for vulnerabilities before returning to the scene of the crime with a more advanced and sophisticated attack strategy. At the end of the day, if you are a cyber defender, the answer is always the same: their motives don't really matter. The more important question you should ask is: Am I prepared?

According to the [CISA](#), good practices to implement immediately to protect against criminal cyber threats include:

- Patching all systems. Prioritize patching known, exploited vulnerabilities;
- Enforcing multifactor authentication;
- Securing and monitoring Remote Desktop Protocol and other risky services;
- Providing end-user awareness and training.

Additionally, organizations should enable DDoS mitigation to protect their network from potential cyberattacks, and web application firewall (WAF) to protect against layer 7 DDoS attacks.

# How many DDoS attacks were there?



Lumen mitigated  
**8,653**

DDoS attacks  
in Q1 2023

**↓6%**

from Q4 2022

**99**

attacks/day

As we wrapped up 2022 with the most attacks that Lumen has mitigated over the past year, Q1 looked to follow the heightened activity on which we have been reporting. Lumen mitigated 8,653 attacks, making Q1 the second busiest quarter we have seen in the past two years. This is only a 6% decrease from last quarter, and a 40% increase year-over-year. On average, Lumen mitigated 99 attacks daily, with Jan. 5 seeing the most attacks (252), followed by Jan. 8 (242).

# How large are the DDoS attacks?

## Largest attack scrubbed

	Dropped bits/s	Dropped pkts/s
<b>Q1 2023</b>	817 Gbps	96 Mpps
<b>Q4 2022</b>	400 Gbps	90 Mpps
<b>QoQ change</b>	<b>↑104%</b>	<b>↑6%</b>
<b>YoY change</b>	<b>↑5%</b>	<b>↓24%</b>

Toward the end of Q4, attacks were appearing to decrease in size. In Q1, however, the largest attack and the average attack size both skyrocketed. The largest attack Lumen mitigated jumped up to 817 Gbps (104% increase quarter-over-quarter) and the average attack increased to 1.8 Gbps — a 40% increase since Q4 and the largest average observed in the past year.

## Bandwidth attacks

- The largest bandwidth attack Lumen mitigated in Q1 was 817 Gbps. This is a 104% quarter-over-quarter increase and a 5% increase over Q1 2022. It is important to note, however, that we mitigated our largest attack to date (over 1 Tbps) in Q2 of 2022. [Learn more](#) about the failed 1 Tbps attack.
- The average attack size was 1.8 Gbps, which is an 40% increase from Q4 and the largest average Lumen has observed over the past year.

## Packet-rate attacks

- The largest packet-rate attack in Q1 was 6% larger than Q4 2022, coming in at 96 Mpps. Despite the increased size over Q4, this is an annual decrease of 24%.
- The average attack size was 354 Kpps — a 13% increase from last quarter.

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.

# 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 represent trends for On-Demand customers, which account for 85% of attacks mitigated in Q1 2023.

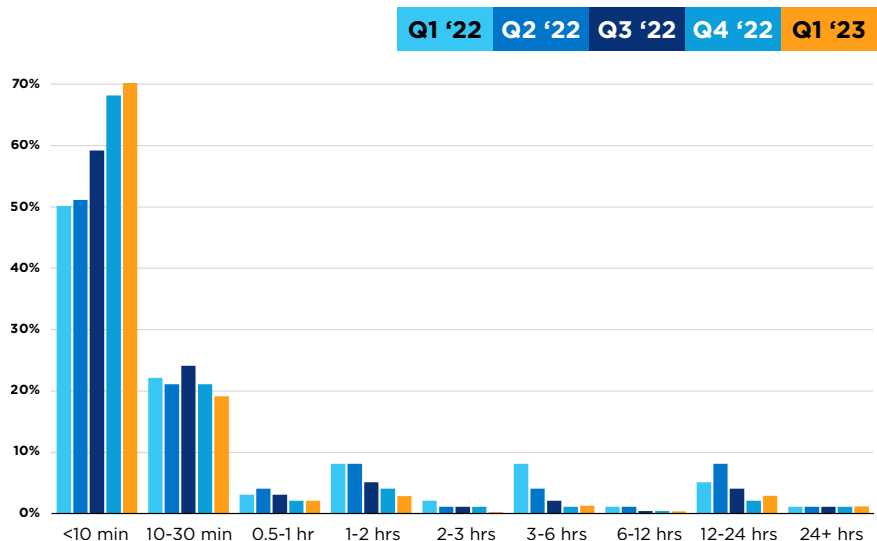
[Do I need On-Demand or Always-On mitigation?](#)

	Q1 2023	QoQ change	YoY change
<b>Median attack duration</b>	8m 21s	↑12%	↓17%
<b>Average attack duration</b>	1h 37m 21s	↑22%	↓38%
<b>Longest attack duration</b>	10 days	-	↑100%

The longest attack period duration we mitigated was 10 days. This does not mean there was a single attack that lasted 10 days; rather, it means there was an active campaign, which could have contained multiple attacks over time.

Additionally, after seeing a trend in which the average attack-period duration decreased in 2022, the average jumped back up in Q1 to over an hour and a half (a 22% increase QoQ). Our most attacked industry continues to be the government sector, with their average attack duration increasing to one hour and twenty-five minutes (48% increase from Q4).

## Distribution by duration



Seventy percent of all attacks on Lumen On-Demand DDoS mitigation customers in Q1 were under 10 minutes. This is a 3% increase from Q4 and a 40% increase year over year. The second most common attack period duration was 10-30 minutes, representing 19% of all activity. This goes to show that threat actors continue to heavily leverage short, quick attacks.



## Distribution by day

Attacks were spread evenly throughout the week. The most popular day for attacks in Q1 was Thursday, which accounted for 17% of activity. Wednesdays and Fridays followed close behind, with 15% each. Saturday showed the lowest activity with 12%.

As we look back at specific dates in Q1, we noticed two clusters of significant attack activity. From Jan. 5-9, Lumen observed a cluster of large attack volumes totaling 994 attacks. These attacks were mostly targeted at a specific customer within the government sector. On the date with the highest number of attacks (252 attacks on Jan. 5), this single customer accounted for 86% of these attacks. Interestingly, this is the week leading up to the Martin Luther King Jr. holiday, which supports our previous theory that attacks are more likely to occur leading up to a holiday.

The second grouping of attacks were from March 28-31, with a total of 740 attacks. Our single government customer from the previous mention was not the main target here, but the most attacked industries during this timeframe were telecommunications followed by government. Unlike the previous grouping of attacks, this cluster was not leading up to a major holiday.

## What do DDoS attacks look like?

### What is a multi-vector attack?

Multi-vector attacks are a combination of attack vectors or techniques to compromise a target network or application. Multi-vector attacks are often more sophisticated and may be more difficult to detect than single-vector attacks. They require a higher level of planning and coordination on the part of the attackers, and they often involve multiple stages or phases. As a result, multi-vector attacks can cause significant damage to the target organization, including data theft, financial loss, and reputational damage.

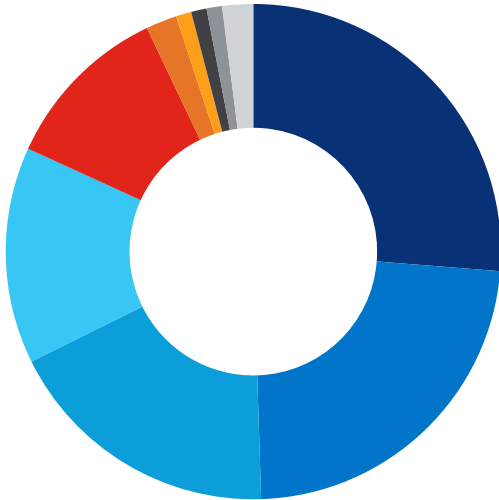
### Multi/single-vector attacks

	Q4 2022	Q1 2023	QoQ change
<b>Multi-vector</b>	39%	44%	↑11%
<b>Single-vector</b>	61%	56%	↓7%

Lumen observed an 11% quarterly increase in multi-vector DDoS attacks; however, single-vector attacks still led, accounting for 56% of activity. While multi-vector attacks accounted for 44% of the attacks we scrubbed, they were more prevalent in the telecommunications (72%) and gaming (56%) verticals.

## Single-vector mitigations

### Top single-vector mitigation type breakdown



			QoQ
DNS	26%	↓9%	
TCP SYN	23%	↓5%	
Static Filtering	18%	↑14%	
UDP	14%	↑24%	
Invalid packets	11%	↑7%	
Other volumetric	2%	↑25%	
TCP ACK	1%	↑654%	
HTTP	1%	↓70%	
SIP	0.9%	↓70%	
Other	2%	↑44%	

While single-vector attacks look consistent with the previous quarter techniques, there is a noticeable shift in single-vector attack methods when compared to 2022.

Domain Name System (DNS) amplification attacks was the most common single-vector attack the second quarter in a row, accounting for 26% of activity. While this was a 9% decrease compared to Q4, it is still a jaw dropping 417% increase year over year. DNS Amplification is used because DNS is essential and cannot be turned off or blocked. Additionally, it provides attackers with a degree of anonymity.

Of all the DNS attacks Lumen mitigated in Q1, the most common form was DNS water torture. The purpose of this type of attack is to overwhelm the resources of an authoritative DNS server, preventing it from responding to valid DNS queries.

Although TCP SYN flooding is the second most common single-vector attack type, the numbers have been decreasing. Since Q4, TCP SYN decreased 5% and accounted for 23% of all single-vector attack activity. Compared to this time last year, TCP SYN decreased 27%. TCP-SYN attacks use spoofed IP addresses — which provide an added level of anonymity — and can also target service ports that cannot be blocked.

The third most common single-vector attack type — with 18% of the total — was static filtering. In Q1, Lumen observed a 14% increase in static filtering over the previous quarter, and a 5% decrease year over year. As mentioned in the previous report, static filtering countermeasures are typically done at the level of ports and protocols.

#### Who is vulnerable to DNS water torture attacks?

Organizations hosting their own public/external DNS infrastructure that responds to DNS queries for their valid domains are potentially vulnerable to DNS water torture attacks. If the same public DNS infrastructure also doubles as a public resolver for internal queries (split-brain DNS), the risk is effectively doubled. A comprehensive DDoS mitigation solution is highly recommended to prevent these attacks from interfering with your business.

## Multi-vector mitigations

### Top multi-vector mitigation type combinations



		QoQ
<b>DNS, TCP SYN</b>	14%	↓30%
<b>DNS, TCP SYN, Static Filtering</b>	8%	↓43%
<b>DNS, Static Filtering</b>	6%	↓47%
<b>DNS Amplification, ICMP, TCP RST, TCP SYN/ACK Amplification, UDP</b>	4%	N.A.
<b>DNS Amplification, ICMP, TCP RST, TCP SYN/ACK Amplification</b>	4%	N.A.
<b>TCP SYN, Static Filtering</b>	4%	↓36%
<b>TCP RST, TCP SYN/ACK Amplification</b>	4%	N.A.
<b>UDP, Static Filtering</b>	3%	↑3%
<b>Other Volumetric, UDP, Static Filtering</b>	3%	↓15%
<b>Invalid Packets, UDP, Static Filtering</b>	1%	N.A.

While the top three multi-vector attacks remained consistent with Q4, we noticed a larger variety of attacks being leveraged across the board.

DNS amplification combined with TCP SYN was the most commonly used vector combination, accounting for 14% of activity in Q1. This was a 30% decrease compared to Q4, and a 13% decrease from Q1 2022. Because both methods leverage ports that cannot be turned off or blocked, defending against this combination requires more sophistication than a simple “deny” rule.

Furthermore, we saw DNS, TCP SYN, and Static Filtering used together in 8% of multi-vector attacks, which is a 43% decrease from Q4. We also saw a variation of this combination, with DNS and Static Filtering accounting for 6% activity (a 47% decrease quarter over quarter).

In addition to the top multi-vector attack combinations, Lumen mitigated a new combination that leveraged six different vectors including DNS Amplification, ICMP, TCP RST, TCP SYN/ACK Amplification and UDP amplification. While each of these vectors targets specific ports and systems of the network, this combination creates a cluster of complexities and intensifies the aggregate bandwidth usage. In some cases of multi-vector attacks, simple filters aren’t sufficient to protection.

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](#)

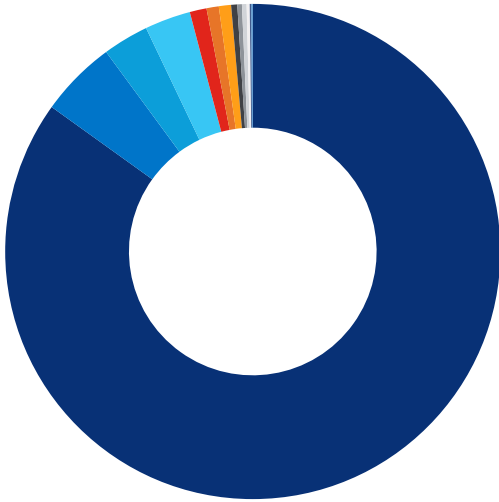
### Misconception: If I protect my network, my applications are not in danger.

While it is important to secure the network infrastructure, modern businesses have become increasingly reliant on applications, which are a prime target for attackers. At Lumen, we have taken a unique approach to threat detection and prevention by using our vast global network as a defense mechanism. Through our proprietary capability called Rapid Threat Defense, we leverage the latest threat intelligence from Black Lotus Labs and incorporate it into our security solutions. This enables us to detect and disrupt potential DDoS attacks within our network in seconds and block them before they ever reach our customers’ environments.

For an [award-winning](#) holistic solution, customers can add an additional layer of security with Lumen Application Protection, which includes Bot Risk Management, and Web Application and API Protection solutions. With this proactive approach, businesses can have peace of mind knowing that their digital assets are safeguarded by one of the largest and most advanced networks in the world.

# Who is being attacked?

## Largest 1,000 attacks by industry



Telecommunications	85%
Other	5%
Gaming	3%
Government	3%
Software & Technology	1%
Finance	1%
Banking	1%
Education	0.4%
Utilities	0.3%
Hosting	0.3%
Manufacturing	0.2%
Transportation	0.1%
Retail & Distribution	0.1%

The 'other' category consists of three customers — a veterinarian clinic, a residential location, and a legal services business.

Of the 1,000 largest attacks Lumen mitigated in Q1, 97% targeted these top five verticals (in order): Telecommunications, Other, Gaming, Government, and Software & Technology.

As we've reported in the past, a single government customer was attacked more than 4,300 times in Q1, representing 50% of all the attacks we mitigated during the quarter. Most of these were small, short, single-vector attacks ranging from 5-10 minutes in duration. Of these, 28% came in the form of DNS attacks and 25% were TCP SYN.

Conversely, the largest attack Lumen mitigated in Q1 came from the telecommunications industry — 817.49 Gbps.

### Telecommunications



85% of the largest 1,000 attacks



Largest bandwidth attack: **817 Gbps**



1,821 total attacks



Largest packet-based attack: **96 Mpps**



Longest attack period duration: **10 days**



**72%** multi-vector attacks

### Other



5% of the largest 1,000 attacks



Largest bandwidth attack: **6 Gbps**



270 total attacks



Largest packet-based attack: **1 Mpps**



Longest attack period duration: **3 days**



**56%** multi-vector attacks

### Gaming



3% of the largest 1,000 attacks



Largest bandwidth attack: **61 Gbps**



89 total attacks



Largest packet-based attack: **22 Mpps**



Longest attack period duration: **5 days**



**56%** multi-vector attacks

## Government



3% of the largest 1,000 attacks



Largest bandwidth attack: **53 Gbps**



5,094 total attacks



Largest packet-based attack: **5 Mpps**



Longest attack period duration: **6 days**



61% single-vector attacks

## Software & Technology



1% of the largest 1,000 attacks



Largest bandwidth attack: **130 Gbps**



344 total attacks



Largest packet-based attack: **13 Mpps**



Longest attack period duration: **9 days**



73% single-vector attacks

### Healthcare industry

While we opened the report with the call out to KillNet targeting the healthcare industry, Lumen did not detect an influx of attacks targeting its healthcare customers. Of the customers observed within this report, however, healthcare represents just 1.1%. Therefore, while this report does not directly reflect the overall attack trends within the healthcare field, Lumen strongly encourages all industries to be well prepared to defend against cybercriminals by implementing DDoS and Application Protection solutions.

## What is the cost of a DDoS attack?

The biggest question you might have while reading through this report is: “Okay, so what’s it going to cost if I’m attacked?” The financial impact of DDoS attacks can vary based on the organization. It is determined by minutes and hours of downtime, the number of IT security staff you have dedicated to security incidents, the volume of customer complaints you must manage, and how much revenue is tied up in your websites and applications.

### Rewind to Q4

In our previous report, we determined that a Software and Technology company that generated \$500 million in online revenue is projected to have a total financial loss of \$20,688,500\* from a DDoS attack. View the previous projection in more detail [here](#).

With that in mind, let’s dive into a hypothetical use case: a mid-size Retail & Distribution company that earns \$152.7 million in total online revenue. Their IT team is on the smaller side, with just three people dedicated to fixing security issues, including responding to DDoS attacks. During a breach they receive about 25 customer support calls per hour.

Based on data from our reports, we expect a company like this to be targeted eight times annually, with an average downtime of 16 hours per attack.

## ThreatX Application and API Protection

# THREATX

ThreatX is managed API and application protection that lets you secure them with confidence, not complexity. It blocks botnets and advanced attacks in real time, letting organizations keep attackers at bay without lifting a finger. Trusted by companies in every industry across the global, ThreatX profiles attackers and blocks advanced risks to protect APIs and applications 24/7.

[Learn more by viewing the ThreatX on Lumen Data Sheet](#)

We anticipate the annual loss for this company is \$2,946,021\*. We found that revenue would be negatively impacted by \$1,830,309, the cost impact from IT operations and customer support to be over \$32,000, and the negative brand impact to the organization to be \$1,068,900. This would be for all eight attacks, ideally, after the first attack an organization would invest in DDoS mitigation services. But these are real numbers that can financially devastate an organization.

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

[Calculate now](#)

## Application Protection

Lumen Application Protection utilizes the best vendors to provide robust application security for our customers. In this report we take a deep dive into the data from one of these partners — [ThreatX](#).

## What application traffic is being blocked?

### ThreatX requests

Non-malicious traffic	58%
Blocked bot traffic	13%
Blocked due to other reasons	29%

Over the past quarter, 42.11% of requests received by ThreatX customers were blocked in real-time. The remaining traffic would be described as non-malicious or normal application traffic.

#### What is a request?

An application request is any instance when an end user attempts to access the application or elements of an application, such as an image or stylesheet. For example, to access to a web page, you typically enter in the URL within a browser's navigation bar and hit 'search' or 'enter'. The browser sends your request to the web page where you will either receive access to the page or be denied access if you do not meet the specifications set forth by the website developers.

You might be wondering why so much traffic was blocked. It is important to note that while ThreatX customers have complete control over their blocking thresholds, specific use cases may require the organizations to block more specific criteria than others. Precise user location, time of day, and user device types are a few examples of how developers can set parameters to determine access to their applications.

For this reason, the percentage blocked does not represent the total number of attacks. Instead, it represents application requests blocked for specific use cases in each application protected by ThreatX.

Of the nearly 25 billion blocked requests, 30.2% [came from bots](#). Some bots are designed to help users navigate the internet and applications, but there are countless other bots, and massive botnets, used with bad intentions. In many cases, malicious bots are designed to gather critical information, attack/disrupt/break APIs, or perform a DDoS attack. According to [ZDNET](#), these malicious bots make up 20% of the world's web traffic. For these reasons, it is highly recommended to implement a comprehensive Bot Risk Management solution to prevent malicious bots from interfering with your business.

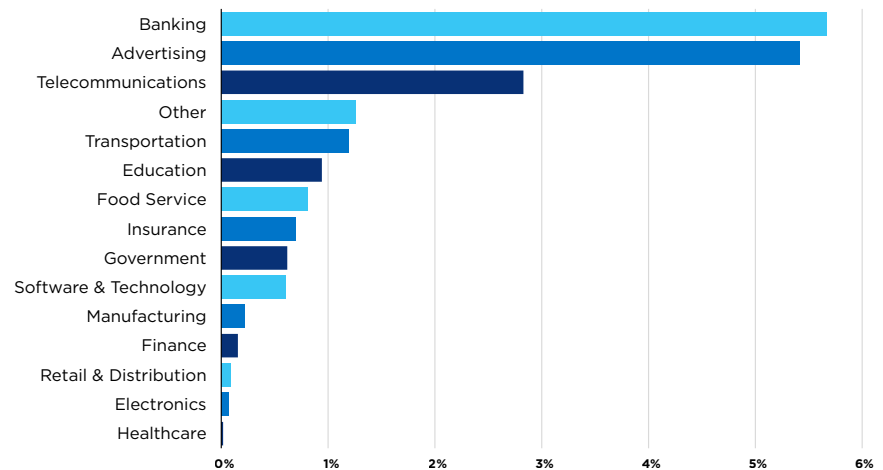
“Of nearly 25 billion blocked requests, 30.2% came from bots. Malicious bots make up 20% of the world's web traffic.”

### Misconception: All bots are malicious...

The term “bot” gets a bad rap, but not all bots are malicious. Did you know that you interact with bots almost every day when you browse the internet? Bad actors often use bots in harmful ways, but they are also very helpful in many of our daily tasks. For example, when you use a search engine, bots manage your request and return a list of search results back to you. To learn more about the differences between good and bad bots, [view this blog](#).

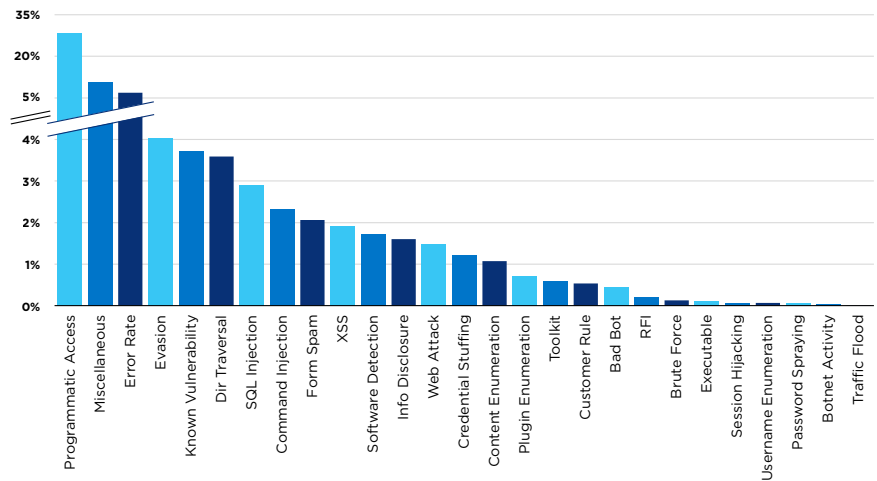
## Blocked traffic by industry

### % blocked API traffic



When we look at the breakdown of blocked traffic by industry over Q1, the banking sector had the highest percentage of blocked traffic at 5.67%, followed closely by the advertising industry at 5.41% and telecom at 2.83%.

# Most blocked application suspicions



As we look into the API traffic that ThreatX monitored, some notable and suspicious activity occurred throughout Q1. The highest percentage of blocked traffic came from programmatic access (28.4%). This is the result of suspicious automated access attempts against a web application. This was followed by 10.55% of blocked miscellaneous attacks, which ThreatX defines as attempts to introduce known malicious code execution in user/user-agent environments. The third most blocked activity came from error rates (6.86%), which are an indication that an offending entity may be performing malicious actions that result in increased HTTP errors returned by the server.

By recognizing the common themes derived from these attacks, you'll be able to detect reconnaissance attempts and thwart potential larger-scale API and application attacks down the line. It is important to implement layers of security which harden the application and API and address potential attackers, ensuring that you stay ahead of the game and remain secure.

As a leader in application and API protection, ThreatX is proud to help protect customers against these threats. Lumen + ThreatX offers comprehensive protection against a wide range of attack types, including programmatic access, error rate, [credential stuffing](#), and more. By leveraging ThreatX's advanced technology, our customers can rest assured their applications are protected against the most common types of attacks.





---

# Final thoughts from Lumen

Cybercriminals will continue to poke and pry at networks and applications to deny service or exploit data, so you need to be well prepared to stand up to any attacks thrown your way. You never know what the next big attack vector will be or which industries will be targeted, but one thing is certain: the best defense is to have a solid in-depth strategy in place.

## Recommendations:

- Nowadays, DDoS mitigation is considered basic cybersecurity hygiene. Just like brushing your teeth prevents cavities, having DDoS mitigation in place can prevent attackers from successfully 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. Then, it's a matter of finding, isolating and removing the malware.
- If your company uses applications to interact with customers, employees, or other stakeholders, then you should have holistic protection against network- AND application-layer attacks. This 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 Risk Management solutions, and pair 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 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 trends we have observed, you can read [our past quarterly reports](#).



## How can Lumen help 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 more than 500 multi-tiered scrubbing locations, Lumen operates 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.

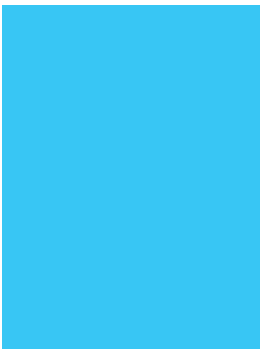
**Need immediate protection? [Lumen® DDoS Hyper®](#) can be ready in minutes.**

**Learn more about our [advanced DDoS Mitigation Service](#).**

## How Can Lumen Help with Application Protection?

With Lumen Application Protection offers an integrated solution that provides application availability, performance, and security in a DevSecOps-friendly environment for rapid, flexible turn-up of protection against multi-vector and mixed application-layer attacks. Lumen partners with a wide variety of Application Protection providers with capabilities spanning web application firewall, bot risk management, and API security to give our customers the optimal selection of features based on their needs.

[Visit our website](#) to see which Application Protection solution fits you best.



\* 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 April 2023 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.

### Methodology

Data in this report is from the timeframe of Jan. 1, 2023 through April 3, 2023.

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 are 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 the attack, then it is counted as a single multi-day period of attack.

Data from ThreatX was derived from an analysis of customer traffic.

