REPORT

Lumen Quarterly DDoS & Application Threat Report

Q4 2023

LUMEN®

Executive Summary

Another year has passed, and it's time to reflect on the lessons learned in 2023. How can we better protect our organizations, employees and customers in 2024?

The purpose of the Lumen Quarterly DDoS & Application Threat Report is to provide you with an overview of the DDoS and application-layer attacks that are targeting organizations and put them into context. Lumen examined data from our Lumen® DDoS Mitigation Service and our API and Application partner, ThreatX, to develop this report.

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

Public sector persecution: Government customers were highly targeted this quarter, experiencing 66% of the largest attacks.

Going out with a bang: Lumen mitigated our largest attack of the year (903 GBits/s) in the final days of 2023.

DDoS drowning: DNS water torture attacks persisted throughout 2023 with no signs of stopping.

AI imaginings: We consider how attackers and defenders will leverage AI in 2024.

2023 by the numbers

Total attacks mitigated:

22,403

Largest bandwidth attack:

903 Gbps

Largest packet rate attack:

202 Mpps

Average bandwidth attack size:

1.75 Gbps

Average packet rate attack size:

423 Kpps

Average attack duration:

2h 40m

Most common single-vector attack methods:

Domain Name System (DNS) Amplification

and

TCP-SYN Flooding

Percentage of attacks that were multi-vector:

38%

Most targeted industries:

- **Telecomm**
- **Government**
- **Software & Technology**

Table of Contents

Year-end trends and predictions

Trends in 2023

Drowning in DDoS attacks

A sinister name for a serious problem — DNS water torture attacks emerged as a trend throughout the year. These attacks flood the Domain Name System (DNS) server with a tsunami of requests, trying to disrupt websites and systems by overwhelming the server. Unlike traditional volumetric DDoS attacks, DNS water torture attacks are more subtle, persistent and low volume from a bandwidth perspective, making them more difficult to detect and automatically mitigate using cloud-based volumetric DDoS protection services. Such attacks are attractive to bad actors, as they can't be blocked outright and require more sophisticated countermeasures.

In the second half of 2023, we saw this type of attack evolve to leverage an unusual technique — DNS over Transmission Control Protocol (TCP) attacks. Typically, DNS queries (and attacks) employ User Datagram Protocol (UDP) as a quick and easy communications protocol. DNS via TCP, meanwhile, requires establishing a TCP session — this is out of the ordinary so it's difficult to block with traditional countermeasures.

We saw a spike in water torture attacks early in the year, and with numbers holding steady across 2023, this vector shows no sign of fading away. Although the attack traffic bandwidth may be small, due to the nature of DNS queries, DNS water torture attacks could have significant packet rates. To protect against DNS water torture attacks, organizations should leverage:

1. A distributed DNS architecture that can absorb the attack traffic
2. Lumen® DDoS Mitigation Service and Lumen® DDoS Appliance Service to mitigate these kinds of attacks

Predictions for 2024

AI for cybersecurity: offense and defense

From the viral popularity of ChatGPT to deepfakes, 2023 was a breakout year for artificial intelligence (AI). It's also the year that the White House issued its executive order on AI, NIST released it AI Risk Management Framework and the European Union reached a provisional agreement on the Artificial Intelligence Act, demonstrating the anxiety around AI standards and how the technology might be abused.

What is Black Lotus Labs®?

BLACK LOTUS LABS® by Lumen

Black Lotus Labs® consists 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, machine learning, and automated threat validation to identify and disrupt the work of malicious actors.

Read the latest threat research

Who is vulnerable to DNS water torture attacks?

Organizations hosting their own 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 doubles. A comprehensive DDoS mitigation solution is highly recommended to maintain business continuity, even under attack.

> “Change is certain and as AI scales the pace of change, encompassing security strategies will be vital.”

One area where AI is already being leveraged for both good and evil is cybersecurity. According to Gartner®, "the use of AI by malicious parties is accelerating the evolution of their attack capabilities and compelling security product leaders to adopt and implement AI technologies more quickly to respond with improved threat detection, investigation and response (TDIR) solutions." In a recent survey by Gartner, "more than 50% of interviewed security providers claimed to already be using machine learning-based AI to enhance threat detection capabilities."[1]

Attackers use AI to:

- Hide from defenders by making their attack sources more difficult to trace
- Automate tasks and anticipate defensive strategies
- Quickly and easily write malware, ransomware and phishing emails

Defenders use AI to:

- Monitor traffic in real time and perform behavioral network analysis to identify traffic patterns and deviations
- Identify potential DDoS attacks before they happen through predictive analytics
- Automate and prioritize DDoS attack investigation and response

If attackers and defenders are already leveraging AI in these ways, then what might 2024 bring? Will AI create new opportunities for faster, smarter, more powerful attacks? Could predictive analytics become even more reliable, driving increased integration with automatic response systems?

AI at the edge

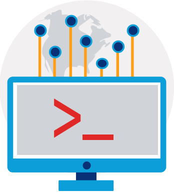
In addition to evolving AI technologies, we must also consider the expanding attack surface. One growing concern in the AI space is how AI might leverage IoT devices for attacks, as well as impact those devices. On the defender side, additional analytics from edge devices might help to further improve AI models for detection, prediction and response.

There are many open questions, but change is certain, and as AI scales the pace of change, encompassing security strategies will be vital.

Black Lotus Labs and AI

Black Lotus Labs, the Lumen threat intelligence team, is at the forefront of defensive AI cybersecurity strategies. This team of security professionals and data scientists leverages proprietary machine learning algorithms over Lumen’s vast dataset to detect patterns in the infrastructure and identify new threats as they emerge — providing our customers with early warnings and buying them lead time.

[1] Gartner, *Emerging Tech: Top Use Cases for AI in Threat Detection, Investigation and Response*, October 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliations in the U.S. and internationally and is used herein with permission. All rights reserved.



Lumen mitigated

4,061

DDoS attacks in Q4 2023

▼4%

from Q3 2023

48

attacks/day

How many DDoS attacks were there?

Seasons change, but cybercrime is evergreen. In Q4 2023, Lumen mitigated 4,061 attacks, holding steady with the number of attacks mitigated the previous quarter (4,217); however, this number represents 56% fewer attacks year over year. On average, we mitigated 48 attacks daily, with November 3rd as our most attacked day of the quarter (154 attacks).

Q4 saw the fewest number of attacks in 2023. Typically, we might expect more attacks in Q4, as bad actors gravitate toward the holidays to group their attacks when many people are out of the office and defenses might be weaker or response times slower. (Read more about this trend in the Q4 2022 DDoS Report, "Timing is everything"). This quarter, however, both Black Friday and Cyber Monday — historically high-attack-activity events — drew in an unremarkable number of attacks (58 and 52, respectively). The fact that attacks took a 4% dip quarter over quarter and a 56% dip from this time last year could suggest that bad actors are exploring different opportunities to inflict damage as defenders have gotten wise to seasonal and holiday-driven attacks.

How large are the DDoS attacks?

Largest attack scrubbed

	Dropped bits/s	Dropped pkts/s
Q4 2023	903 Gbps	114 Mpps
Q3 2023	485 Gbps	121 Mpps
QoQ change	▲86%	▼6%
YoY change	▲126%	▲26%

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.

After a sizeable 817 GBits/s attack in Q1 of 2023, attack sizes shrank each quarter throughout the year until Q4, which saw a whopping 903 GBits/s attack — the largest attack of 2023. This represents an 86% increase in attack size compared to the previous quarter and a 126% increase year over year.

This considerable attack targeted a Telecomm customer, which is in line with the trends we've seen in previous quarters. Telecomm is a frequently attacked vertical, as these customers carry traffic for all other industries. The industry attracts large attacks, as a successful breach could compromise large amounts of sensitive data. It's likely that the intended target of this attack was not the Telecomm company itself but one or several of its customers.

How long are DDoS attacks lasting?

	Q4 2023	QoQ change	YoY change
Median attack duration	10m 0s	-	↑35%
Average attack duration	3h 16m 56s	↓21%	↑121%
Longest attack duration	7 days	↑16%	↓30%

Attack duration numbers are affected by the customer's mitigation model. There are two options:

1. **On-Demand mitigation:** Traffic is always monitored, but only scrubbed once a threat has been detected.
2. **Always-On mitigation:** Traffic is constantly scrubbed to further minimize downtime.

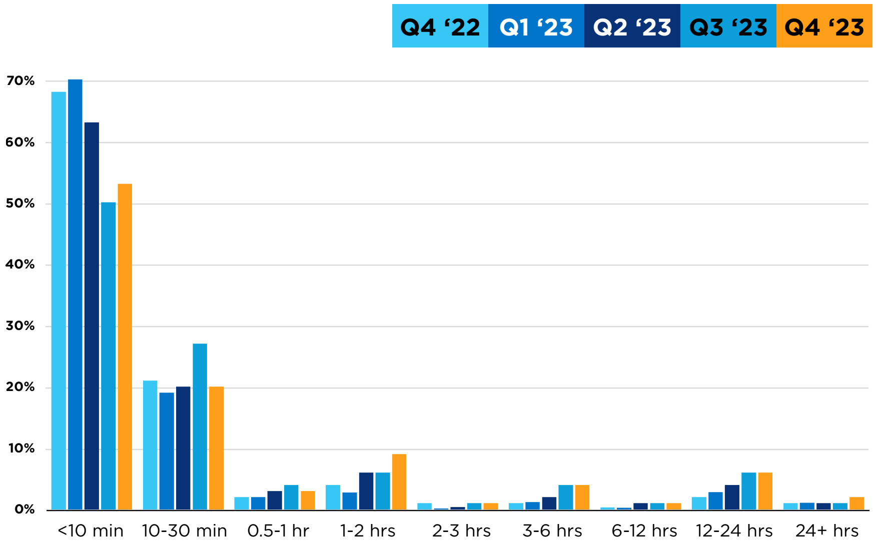
The data points in this section only portray trends for On-Demand customers, which account for 73% of attacks mitigated in Q4 2023.

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

The longest attack period duration we mitigated was seven days — meaning there was an active campaign over seven days, which could have contained multiple attacks over that period. This increased 16% from Q3 but marks a 30% decrease year over year.

Despite a small dip quarter over quarter, average and median attack-period durations increased over the year. Our average attack duration more than doubled annually, jumping from ~1.3 hours to over three hours in Q4 2023.

Distribution by duration



> “While shorter attacks are more common, we did see a trend this year of longer attacks.”

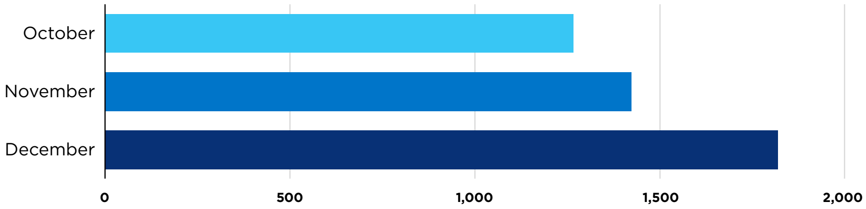
Seventy-three percent of attacks on Lumen On-Demand DDoS Mitigation customers in Q4 clocked in at under 30 minutes, with 53% of those attacks under ten minutes — our most common attack-period duration. While shorter attacks are more common, we did see a trend this year of longer attacks — 89% of all attacks were under 30 minutes a year ago compared to 73% this quarter.

Distribution by day

For the most part, attacks were spaced evenly throughout the days of the week, with a small preference for Friday (17% of all attacks). Cybercriminals’ penchant for TGIF doesn’t appear to represent a trend, however. This number aligns with Friday November 3rd, the day of the quarter that saw the most attacks thanks to a targeted Telecomm attack campaign (154 attacks on November 3rd compared to the Q4 daily average of 48 attacks).

We expected the ecommerce events of Black Friday and Cyber Monday to draw more attacks in Q4, as well as the weeks leading up to major holidays of Thanksgiving and Christmas. However, these events saw an average number of attacks, indicating a shift in bad-actor tactics.

Distribution by month



Two multi-day clusters of attacks in mid and late December meant that December contained the most attack activity with 1,807 attacks. Although November 3rd was the most-attacked day of the quarter, when we zoom out, we see that the number of attacks ramped up over time with October seeing the fewest attacks.

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.

Learn more

What do DDoS attacks look like?

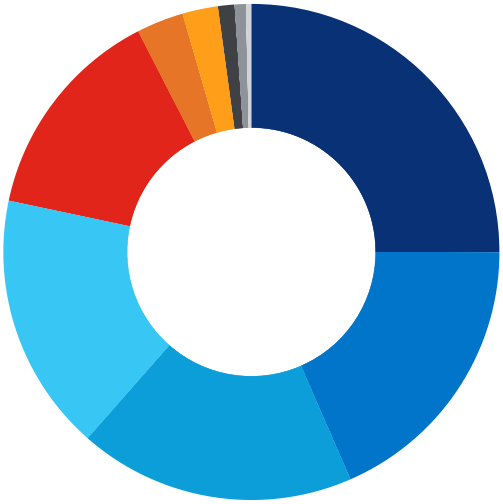
Multi/single-vector attacks

	Q3 2023	Q4 2023	QoQ change
Multi-vector	35%	32%	↓7%
Single-vector	65%	68%	↑4%

Throughout 2023, the percentage of multi-vector attacks compared with single-vector attacks trended downward — from 44% multi-vector attacks in Q1 and Q2 to 35% in Q3 and 32% in Q4. By industry, multi-vector attacks remained prevalent in Telecomm (46%) but dropped off precipitously in Gaming (28%) — an industry that historically has experienced more than 50% multi-vector attacks. Despite an anomalous surge in multi-vector attacks in Banking last quarter, 23% of attacks were multi-vector in Q4. Retail & Distribution, however, which has in past quarters had mostly single-vector attacks, jumped up nearly 300% QoQ to 37% multi-vector attacks. This is likely due to a shift to more complex attacks on Retail during the holiday spending season.

Single-vector mitigations

Top single-vector mitigation type breakdown



			QoQ
🟦	**Static filtering**	25%	↑23%
🟦	**DNS**	18%	-
🟦	**TCP SYN**	18%	↑3%
🟦	**Invalid packets**	17%	↓14%
🟥	**UDP**	14%	↓19%
🟧	**Other volumetric**	3%	↑58%
🟨	**SIP**	2%	↑166%
⬛	**HTTP**	1%	↑61%
◼	**per_connection_flood_protection**	1%	↓39%
⬜	**dns_auth**	0%	↓67%.

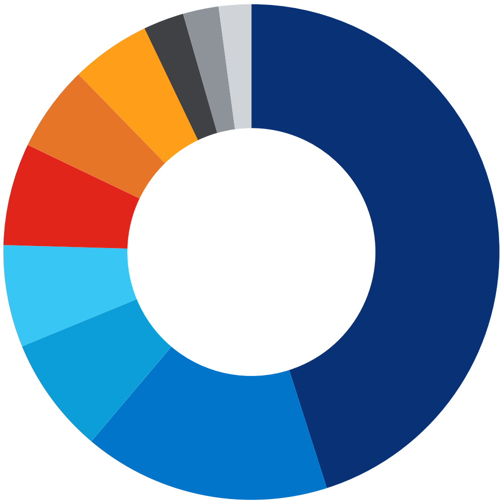
Twenty-five percent of single-vector attacks in Q4 were fairly straightforward to mitigate with static filtering countermeasures, which are typically done on items such as port and protocol. These statistics also include known bots and abused reflectors as discovered by Black Lotus Labs, which provides initial mitigation against attacks.

DNS and TCP SYN each accounted for 18% of single-vector attack activity for the quarter. The vast majority of attacks in Q4 were against Government customers, and TCP SYN and DNS attacks were the top single-vector types used against this sector, which is consistent for this vertical.

Indeed, DNS attacks were prevalent throughout the year, as noted in the trends section on page 5 of this report. Invalid packets remain a popular attack type (17%) as well as UDP (14%), although both types dipped in Q4 compared to the last two quarters.

Multi-vector mitigations

Top multi-vector mitigation type combinations

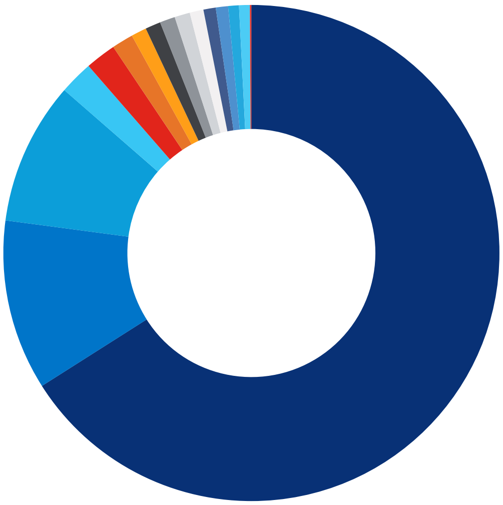


			QoQ
■	**DNS, TCP SYN**	33%	▲118%
■	**DNS, TCP SYN, static filtering**	12%	▲47%.
■	**DNS, static filtering**	6%	▼7%
■	**Invalid packets, static filtering**	5%	▼7%
■	**TCP SYN, static filtering**	5%	▲102%
■	**UDP, static filtering**	4%	▲2%
■	**Invalid packets, UDP**	4%	-
■	**Invalid packets, TCP SYN**	2%	▲56%.
■	**DNS, TCP SYN, UDP**	2%	▲1133%.
■	**Invalid packets, UDP, static filtering**	2%	▼25%

Every quarter of the year saw DNS amplification and TCP SYN flooding as the top vector combination; however, in Q4 the attack combination more than doubled from 15% to 33% of activity. This represents a 58% increase YoY. These are both volumetric attack methods that provide an added layer of anonymity to the attacker. And both exploit vulnerabilities that cannot be blocked or turned off (DNS and service ports, respectively), making the difficult-to-defend combination attractive to attackers.

Defending against multi-vector attacks is complicated — the more vectors used, the more countermeasures needed to mitigate the attack. Whereas, with a single-vector attack, defense could be as straightforward as a "deny" rule. For proper mitigation, organizations should consider combining DDoS Mitigation with Application Protection for a holistic defense strategy.

Learn more



Who is being attacked?

Largest 1,000 attacks by industry

🟦	**Government**	66%
🟦	**Software & Technology**	11%
🟦	**Telecomm**	9%
🟦	**Finance**	2%
🟥	**Gaming**	2%
🟧	**Other**	1%
🟧	**Banking**	1%
⬛	**Media & Entertainment**	1%
◼	**Retail & Distribution**	1%
◻	**Insurance**	1%
⬜	**Manufacturing**	0.9%
🟦	**Business Services**	0.8%
🟦	**Utilities**	0.8%
🟦	**Education**	0.7%
🟦	**Hosting**	0.7%
🟥	**Healthcare**	0.1%

Of the 1,000 largest attacks Lumen mitigated in Q4, 90% targeted these five top verticals (in order): Government, Software & Technology, Telecomm, Finance and Gaming. Historically, Telecomm tops this list, experiencing 74% and 85% of the largest 1,000 attacks in Q2 and Q1, respectively. This is due to the nature of the Telecomm industry, which transmits and stores copious amounts of sensitive data for millions of customers. This quarter, Telecomm was still highly targeted, experiencing many of the largest attacks of Q4, including the largest attack of 2023.

However, this quarter we witnessed something new — the Government sector was our top targeted vertical, receiving 66% of the 1,000 largest attacks Lumen mitigated. This is a significant deviation from past quarters, representing a 163% increase from Q3 and a considerable 4025% uptick year over year.

One customer accounted for 1,759 attacks of the 1,953 government attacks in Q4, of which 20% were automatically blocked by static filtering countermeasures. The main vectors used were DNS and TCP SYN. Although these attacks were relatively small, the fact that someone carried out a targeted campaign of such volume against one customer over a quarter is significant, and we've observed this trend throughout the year.

About 25% of all Q4 attacks were assisted by Lumen® Rapid Threat Defense for mitigation, with these customers benefitting directly from Lumen Black Lotus Labs proprietary threat intelligence. Time matters to your business, and by detecting bad actors faster, Lumen protects customers sooner.

ThreatX API and Application Protection

THREATX

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, command injection, credential stuffing, evasion and more. By leveraging ThreatX's advanced technology, our customers can rest assured their applications are protected against the most common types of attacks.

Learn more by viewing the ThreatX on Lumen Data Sheet

Application protection

Lumen Application Protection uses industry-leading 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.

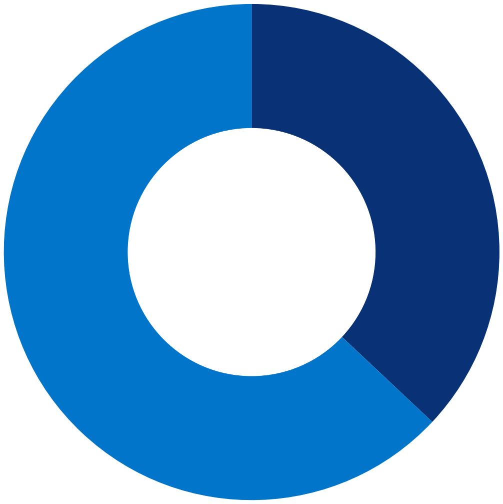
What application traffic is being blocked?

ThreatX requests

	Q4 2023
Total requests	84.8 Billion
API requests analyzed	57.9 Billion
Total blocked requests	1.7 Billion
Total match events	1 Billion

Percentage of blocked traffic that was malicious

■	**Blocked bot traffic**	37%
■	**Blocked due to other reasons**	63%



In Q4 2023, ThreatX customers received more than 84.8 billion requests to their applications, the majority of which were application program interface (API) requests. APIs pose a unique security risk. They connect various applications so they can share data, which exposes valuable business logic, and since they exist to be easily integrated and operate behind the scenes, there are inherent vulnerabilities. All this combined with the rapid proliferation of APIs means they are increasingly targeted by attackers.

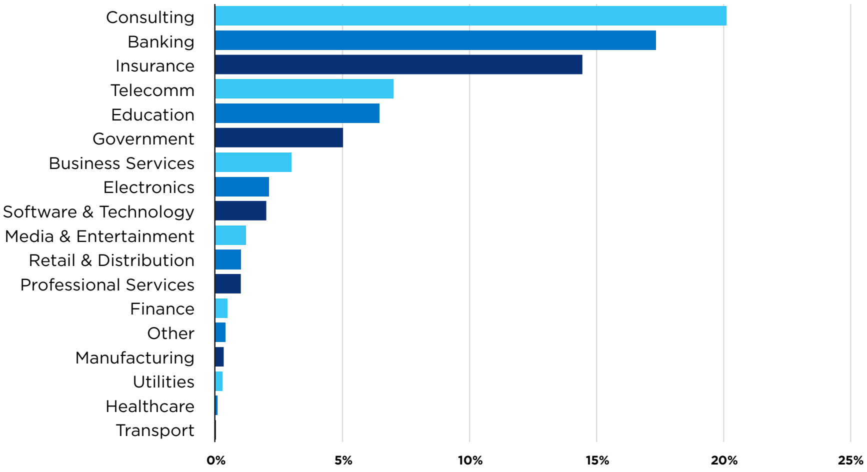
About 2% of total application requests were blocked in real time, and almost 37% of that blocked traffic was from bots. That leaves 63% of malicious traffic that was blocked due to other reasons, which could include anything from a targeted attacker trying to exploit a known vulnerability to a geographic-based blocker if a company doesn't do business in a certain region.

Match vs Block

A match is an event where ThreatX detects a suspicious request to an application but does not block it immediately. Instead, it assigns a risk score to the request and tracks it over time. A block is an event where ThreatX blocks a known malicious request, preventing an attack from reaching the application. A match can lead to a block if the risk score accumulates over multiple requests, or the risk score may decrease if the request is normal.

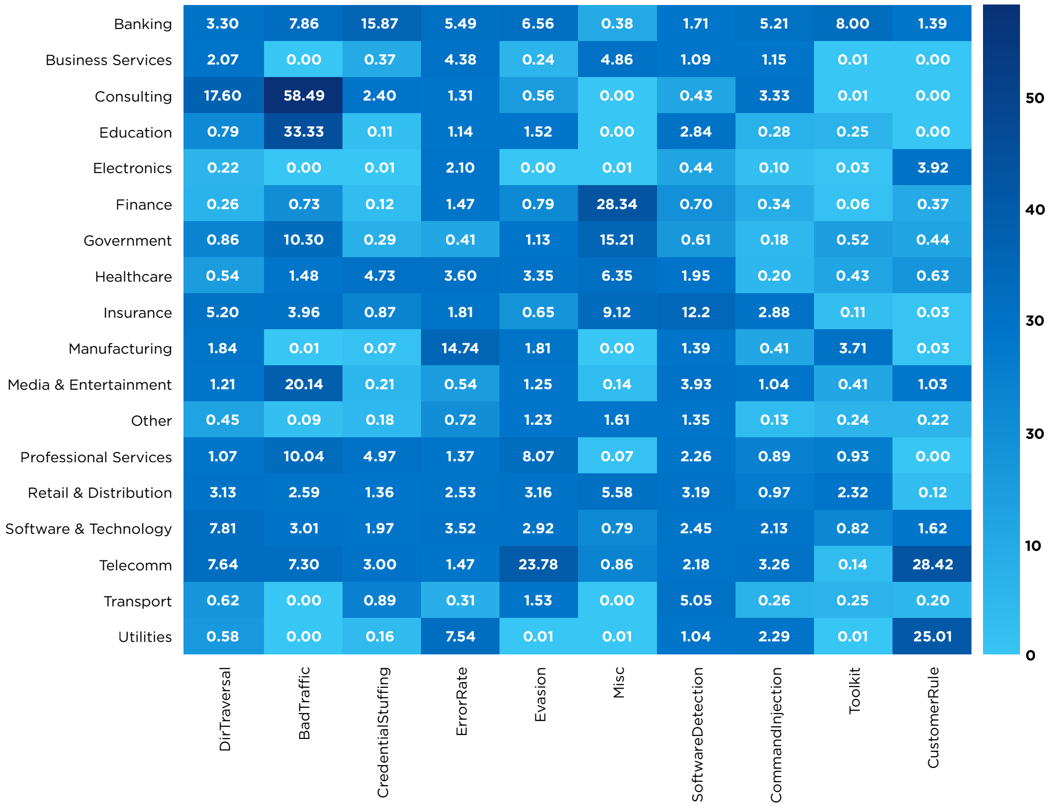
Blocked API traffic by industry

Attack ratio by industry



Looking at the blocked API traffic by industry in Q4, we see that the Consulting sector had the highest block rate (20%) followed by Banking (17%), Insurance (14%) and Telecomm (7%). This is not that surprising considering the highly valuable data at play in each industry, such as financial information. The public sector, which had the sixth-highest blocked API traffic ratio, was a particularly interesting case study in Q4 — exhibiting an uptick in attacks, illustrated by the large number of blocks and the high match percentage. This data suggest that there may have been persistent, focused attacks on government applications throughout the quarter, as high match and block rates indicate that an attacker could be testing an application's defenses.

Top attack vectors by industry



	DirTraversal	BadTraffic	CredentialStuffing	ErrorRate	Evasion	Misc	SoftwareDetection	CommandInjection	Toolkit	CustomerRule
Banking	3.30	7.86	15.87	5.49	6.56	0.38	1.71	5.21	8.00	1.39
Business Services	2.07	0.00	0.37	4.38	0.24	4.86	1.09	1.15	0.01	0.00
Consulting	17.60	58.49	2.40	1.31	0.56	0.00	0.43	3.33	0.01	0.00
Education	0.79	33.33	0.11	1.14	1.52	0.00	2.84	0.28	0.25	0.00
Electronics	0.22	0.00	0.01	2.10	0.00	0.01	0.44	0.10	0.03	3.92
Finance	0.26	0.73	0.12	1.47	0.79	28.34	0.70	0.34	0.06	0.37
Government	0.86	10.30	0.29	0.41	1.13	15.21	0.61	0.18	0.52	0.44
Healthcare	0.54	1.48	4.73	3.60	3.35	6.35	1.95	0.20	0.43	0.63
Insurance	5.20	3.96	0.87	1.81	0.65	9.12	12.2	2.88	0.11	0.03
Manufacturing	1.84	0.01	0.07	14.74	1.81	0.00	1.39	0.41	3.71	0.03
Media & Entertainment	1.21	20.14	0.21	0.54	1.25	0.14	3.93	1.04	0.41	1.03
Other	0.45	0.09	0.18	0.72	1.23	1.61	1.35	0.13	0.24	0.22
Professional Services	1.07	10.04	4.97	1.37	8.07	0.07	2.26	0.89	0.93	0.00
Retail & Distribution	3.13	2.59	1.36	2.53	3.16	5.58	3.19	0.97	2.32	0.12
Software & Technology	7.81	3.01	1.97	3.52	2.92	0.79	2.45	2.13	0.82	1.62
Telecomm	7.64	7.30	3.00	1.47	23.78	0.86	2.18	3.26	0.14	28.42
Transport	0.62	0.00	0.89	0.31	1.53	0.00	5.05	0.26	0.25	0.20
Utilities	0.58	0.00	0.16	7.54	0.01	0.01	1.04	2.29	0.01	25.01

BadBot vs BadTraffic

BadBot attacks come from known BadBots such as Mirai or bot traffic that ThreatX has determined to be malicious based on its actions. BadTraffic is usually HTTP traffic that does not meet the standard specifications of the HTTP protocol, such as mismatching headers and values and invalid or unexpected characters.

Programmatic access attacks were removed from the dataset to avoid skewing the heat map. Miscellaneous attacks include match events that do not fit in other categories, such as matching on traffic that is specific to the context of a customer's business use cases, i.e., restricting access to certain parts of the application.

Going a layer further, when you look at the heat map showing attack trends by industry, you can see some interesting patterns. For example, Consulting and Education were both highly attacked by BadTraffic, indicating substantial traffic from known malicious sources, such as an invalid HTTP request. Telecomm, on the other hand, experienced a high rate of attacks that matched custom policies created by the customer. High CustomerRule matches imply targeted attacks against this sector.

These trends show a diverse and complex threat landscape and highlight the need for security solutions that are tailored by industry.

Programmatic Access

The ability to manage, control, and interact with a web application or its resources through automated processes, typically by using APIs or scripts, rather than through a user interface.

DirTraversal

DirTraversal, or Directory Traversal, attacks attempt to access files and directories that are stored outside the web root folder.

BadTraffic

Anomalous traffic such as a malformed request, for example, HTTP smuggling.

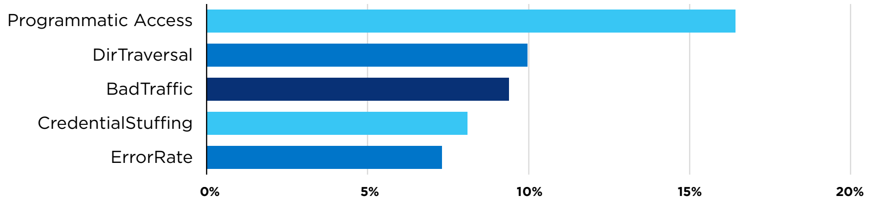
CredentialStuffing

The use of automated tools to try large numbers of username/password combinations, often obtained from previous data breaches, to gain unauthorized access to user accounts.

ErrorRate

Attacks that intentionally induce errors in applications at a rate that overwhelms the system, designed to either exhaust system resources, degrade performance, disrupt service, or expose vulnerabilities.

Top 5 blocked application suspicions



Of the different attack vectors ThreatX monitored throughout the quarter, the highest percentage of blocked traffic came from:

- Programmatic Access (16.43%)
- DirTraversal (9.97%)
- BadTraffic (9.39%)
- CredentialStuffing (8.09%)
- ErrorRate (7.3%)

It's important to note that programmatic access requests, while suspicious, are not always malicious, so it's typical for this suspicion to top the list. Although it didn't make the top five application suspicions, Q4 2023 also saw a lot of BadBot activity across nearly all industries. This bot-related traffic could look very similar to BadTraffic and have the same goals (data theft, fraud or even user experience issues). Banking and Governments sectors in particular experienced heavy BadBot and BadTraffic application attacks, indicating the need for robust monitoring and filtering mechanisms to manage volumetric threats.

While the top five blocked suspicions err on the volumetric side of the attack spectrum, sophisticated and subtle attacks were also prevalent this quarter. SQL injection, which can cause data breaches or compromise systems, was leveraged against several sectors with critical, sensitive data, including Education, Finance and Government. XSS or Cross-site scripting, which can hijack user sessions or redirect to malicious sites, was significantly higher in Business Services, Consulting, Insurance, Retail & Distribution and Telecomm. These sectors might have web applications that are more exposed or vulnerable to XSS due to the nature of their online services. Both attack types require enhanced application-layer security measures to mitigate.

Cybersecurity is a moving target—the data reveal a staggering range of attack vectors, employed in different ways across different industries. By recognizing the common themes derived from these attacks, you'll be able to detect reconnaissance attempts and thwart potential large scale API and application attacks down the line. It is important to implement layers of security such as Web Application & API Protection (WAAPs) to help identify and block the tailored threats aimed against your organization and industry.

Lumen + ThreatX offers comprehensive protection against a wide range of attack types, including programmatic access, credential stuffing, evasion and more. By leveraging ThreatX's advanced technology, our customers can rest assured their applications are protected against the most common types of attacks.

Conclusion and recommendations

Looking back on 2023, it's clear that attack trends evolve rapidly, even quarter over quarter. It's imperative that defense strategies evolve just as quickly, and that all organizations fortify their security postures by partnering with best-in-class providers.

Recommendations:

- DDoS mitigation is considered basic cybersecurity hygiene. Just like brushing your teeth to avoid 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 help 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.

If you want to learn more about trends we've observed, read our past quarterly reports.

Texas Rangers' World Series triumph backed by Lumen DDoS protection

Read our exciting news

How can Lumen help with DDoS mitigation?

With one of the largest DDoS mitigation deployments in the industry, backed by 170 Tbps of network-based mitigation capacity enacted at more than 500 multi-tiered scrubbing locations, Lumen operates DDoS mitigation at scale. You 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 can also take advantage of our 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.

Methodology

Data in this report are from the timeframe of October 1, 2023, through December 31, 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.

This information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk. Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice.