REPORT

Lumen Quarterly DDoS & Application Threat Report

Q2 2023

LUMEN®
The Platform for Amazing Things℠

Executive Summary

DDoS

- An overview of Qakbot
- Attack sizes, lengths, and frequencies
- Attack vectors
- Targeted industries

Application Threats

- Blocked application traffic
- Blocked API traffic by industry
- Top 5 blocked application suspicions

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:

Qakbot — a persistent and evolving threat: Qakbot has established itself as a prominent threat in the cyber landscape and continually evolves with advanced attack vectors. Organizations should remain well protected and on high alert from this malware.

Industry targets: Among the top 1,000 largest attacks mitigated in Q2 2023, the telecommunications and government sectors were the most targeted.

Multi-vector attacks — a growing trend: Multi-vector attacks, combining various attack techniques, are becoming more prevalent. In Q2 2023, 44% of DDoS attacks were multi-vector, requiring advanced mitigation strategies to counter the complex threat landscape posed by these attacks.

API traffic growth: As businesses continue to adopt APIs, there has been a significant rise in API traffic. We expect this trend to continue, necessitating robust API protection solutions to safeguard against potential attacks exploiting API vulnerabilities.

LUMEN®

Table of Contents

LUMEN®

Introduction

The cybersecurity landscape is always evolving, with threat actors constantly adapting their techniques to stay ahead. One such threat that has caught the attention of security professionals is known as Qakbot, aka Pinkslipbot or Qbot.

What is Qakbot?

Qakbot has established itself as a prominent threat in the cyber landscape, with origins dating back to 2007. It is a sophisticated **banking trojan** that has undergone an astonishing transformation into a malware distribution service, demonstrating advanced **obfuscation techniques** and employing new attack vectors. It has adapted its tactics to evade traditional security measures, making it increasingly challenging to detect and mitigate its activities.

Banking Trojan

Malware designed to collect online banking credentials and other sensitive information from infected machines.

Obfuscation techniques

Obfuscation Techniques refer to the capabilities to operate the botnet undetected or less likely to be detected, and extract the data or perform malicious actions against the target in a manner that avoids detection.

Who is controlling Qakbot

Tracking organizations believe there may be two organizations controlling Qakbot. The operators are known as "Mallard Spider" by some tracking organizations, and "Gold Lagoon" by others, yet various tracking orgs use both names. In addition, other groups have repurposed or even leased the malware.

Tracking Qakbot

Leveraging the visibility of the Lumen global network and employing advanced techniques such as behavioral analysis and machine learning, Lumen Black Lotus Labs® has gained crucial insights into Qakbot's evolving tactics, techniques and procedures.

In December 2022, Black Lotus Labs observed several spamming campaigns leveraging macro-based exploitation of Microsoft Office documents. In response to security measures, Qakbot operators pivoted away from this tactic. When they launched their next campaign in early 2023, they were prepared with three new exploits so that when one became known to defenders, they could quickly leverage another. This was a case of being prepared in advance, and it was very effective for the attackers.

Additionally, Qakbot has been seen repurposing victim machines into **command and control servers (C2s)**. In a recent Black Lotus Labs blog post, the team "observes that more than 25% of C2s don't remain active for more than a day, and 50% don't remain active for more than a week. We see Qakbot continue to replenish the supply of C2s through bots that subsequently turn into C2s." These short-lived C2s contributed to the broader botnet ecosystem, which Qakbot operators leveraged to target other organizations. This interconnectedness of cyberthreats emphasizes the need for comprehensive defenses to protect your organization and the wider digital community.

Command and Control (C2)

C2s allow cybercriminals to remotely control and manage compromised computer systems — often as part of a larger botnet — to carry out malicious activities such as launching attacks, stealing data and spreading malware.

Who is at risk?

Qakbot attacks pose a risk to a wide range of individuals and organizations. While the malware predominantly targeted financial institutions in the past to harvest online banking credentials and sensitive information, the malware has pivoted to focus on being a malware distribution service, so many other industries are now being targeted.

Healthcare industries should be on the lookout for Qakbot attacks, as malware infections can significantly impact healthcare systems, leading to disruptions in patient care and potentially endangering lives. Qakbot's ability to steal sensitive healthcare data — including patient records and medical information — poses a severe threat to patient privacy and can lead to identity theft or medical fraud.

Another potential target is manufacturing. Qakbot attacks on the manufacturing sector can disrupt production processes, leading to operational downtime and financial losses. Manufacturers often rely on interconnected systems and supply chains, making them susceptible to malware infections that can compromise production lines, steal intellectual property, and disrupt logistics. Qakbot attacks can lead to the loss of proprietary information, trade secrets, and sensitive data, impacting the competitiveness and reputation of manufacturing companies.

While the healthcare and manufacturing industries have not been exposed to substantial Qakbot attacks since 2020, it is advised that they should continue to remain on high alert for potential attacks by Qakbot and other similar malware.

As for the sizes of organizations at risk, Qakbot has no exceptions. The potentially weaker cybersecurity defenses of small- and medium-sized enterprises open the door for potential Qakbot attacks, while large enterprises and corporations are at risk due to Qakbot's adaptability and persistence, which can result in data breaches and operational disruptions.

Where does this threat intelligence come from?

BLACK LOTUS LABS® by Lumen

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

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

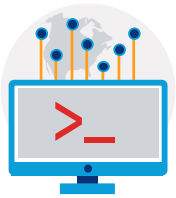
Stopping Qakbot

What distinguishes Qakbot is its ability to constantly reinfect and recycle itself within compromised networks. It updates its C2 infrastructure regularly, rendering traditional security solutions ineffective in tracking and disrupting its communication channels.

To counter the evolving threats posed by Qakbot, organizations must adopt proactive cybersecurity practices. Best practices to mitigate Qakbot attacks include:

- deploy and monitor phishing countermeasures;
- train employees to recognize phishing emails;
- run modern endpoint detection software and be continually investigating alerts and data for signs of compromise;
- and monitor/protect outbound traffic from communications to known qakbot C2s.

For more information on Lumen's latest Qakbot discoveries, review the Black Lotus Labs blog titled "Qakbot: Retool, Reinfect, Recycle."



Lumen mitigated

5,472

DDoS attacks in Q2 2023

▼37%

from Q1 2023

63

attacks/day

How many DDoS attacks were there?

When Q2 2023 began, it was after two quarters in a row with a relatively high number of mitigated DDoS attacks. We ended the quarter with 5,472 attacks mitigated — a 37% decrease from Q1. When we compare this number to last year, however, it remains higher overall with a 20% increase year-over-year. On average, Lumen mitigated 63 attacks daily, and April 1-4 saw the most activity with a combined total of 748 attacks.

How large are the DDoS attacks?

Largest attack scrubbed

	Dropped bits/s	Dropped pkts/s
Q2 2023	711 Gbps	201 Mpps
Q1 2023	817 Gbps	96 Mpps
QoQ change	▼13%	▲111%
YoY change	▼5%	▼18%

LUMEN®

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.

In the first quarter of 2023, we saw a large spike in the largest attack Lumen scrubbed. In Q2, the largest attack decreased 13% (711 Gbps), but the dropped packets increased 111% (201 Mpps).

Bandwidth attacks

- In Q2, the largest bandwidth attack Lumen mitigated was 13% smaller than the previous quarter for Gbps dropped (711 Gbps), This is a 5% decrease in the Gbps dropped year-over-year.
- The average attack size was 1.9 GBits, — a 6% increase over Q1 and the largest average Lumen has observed over the past year.

Packet-rate attacks

- The total number of dropped packets since last quarter increased 111% (201 Mpps). This drastic change in packets dropped may be a result of **DNS water torture attacks** this quarter. These attacks sometimes spike, so it is important for companies to be prepared. When comparing the number of dropped packets to last year, we noticed an 18% decrease year-over-year.
- The average attack size was 838 Kpps — a 137% increase from Q1 and the largest average Lumen has observed over the past year.

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 76% of attacks mitigated in Q2 2023.

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

How long are DDoS attacks lasting?

	Q2 2023	QoQ change	YoY change
Median attack duration	8m 55s	▲7%	▼11%
Average attack duration	2h 5m 10s	▲29%	▼40%
Longest attack duration	7 days	▼30%	▼67%

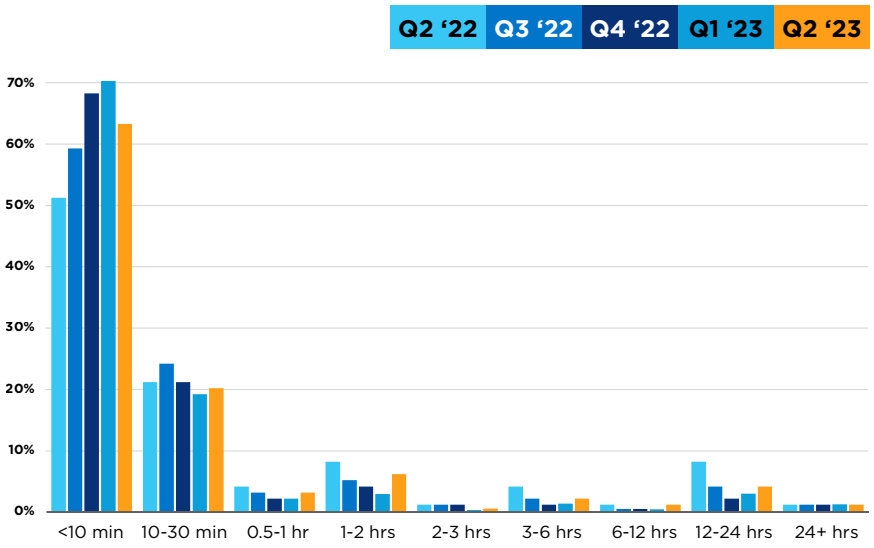
The longest attack-period duration we mitigated was seven days. This does not mean there was a single attack that lasted seven days; rather, it means there was an active campaign, which could have contained multiple attacks over time.

Additionally, the average attack period is trending upward as we noticed another quarter of increased attack durations. The average attack period increased 29% to just over two hours.

As we look into the most attacked industries, the government sector continues to be the top target. The average attack duration within the government sector increased to two hours and twenty minutes (64% increase from Q1).

.

Distribution by duration



Sixty-three percent of all attacks on Lumen On-Demand DDoS mitigation customers in Q2 were under 10 minutes in duration. This is an 11% decrease from Q1 and a 23% increase year over year. The second most common attack-period duration was 10-30 minutes, representing 20% of all activity. This goes to show that threat actors continue to heavily leverage short, quick attacks.

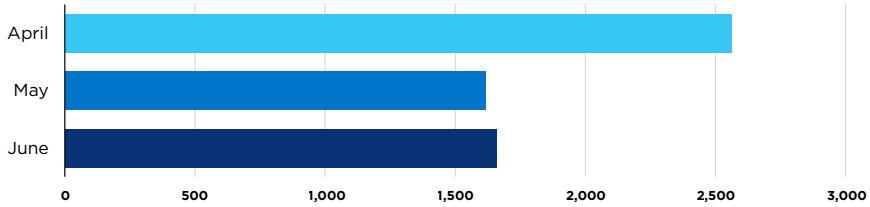
Distribution by day

Attacks were spread evenly throughout the week. The most popular day for attacks in Q2 was Wednesday, which accounted for 18% of activity. Monday followed close behind, with 17%. Friday showed the lowest activity with 11%.

As we look back at specific dates in Q2, we noticed a cluster of significant attack activity. From April 1-4, Lumen observed large attack volumes totaling 748 attacks. While we expected to see the finance vertical being impacted at this time; instead, these attacks were mostly targeted at a specific customer within the government sector. Lumen mitigated 433 attacks for this customer alone.

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.

Distribution by month



As we zoom out and view Q2 by month, we notice that April contained the most attack activity with 2,561 total attacks. We then saw a decrease in the total number of attacks in May with 1,617. May also contained the fewest attacks throughout the entire quarter. And in June, attacks slightly increased to a total of 1,658.

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.

What do DDoS attacks look like?

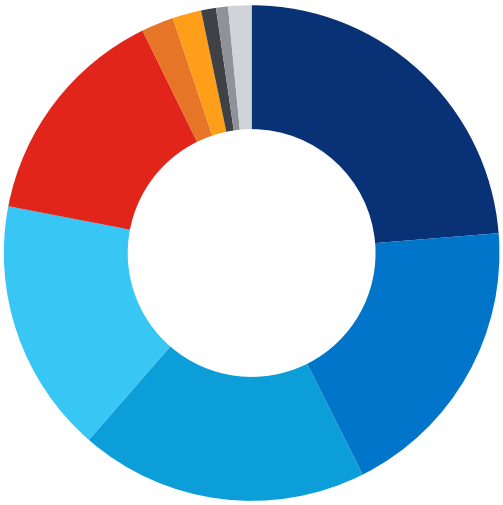
Multi/single-vector attacks

	Q1 2023	Q2 2023	QoQ change
Multi-vector	44%	44%	-
Single-vector	56%	56%	-

In Q2, multi-vector and single-vector DDoS attacks remained consistent at 44% and 56% respectively. While multi-vector attacks accounted for 44% of the attacks we scrubbed, they continue to be more prevalent in the telecommunications and gaming verticals, accounting for 60% for each.

Single-vector mitigations

Top single-vector mitigation type breakdown



		QoQ
Static filtering	24%	↑30%
UDP	19%	↑35%
Invalid packets	19%	↑79%
TCP SYN	17%	↓29%
DNS	15%	↓44%
Other volumetric	2%	↓4%
IP fragmentation	2%	↑282%
SIP	1%	↑10%
HTTP	1%	↓14%
Other	2%	N.A..

In Q2, we observed a shift in the single-vector attack methods being used.

With a 44% decrease from the previous quarter, Domain Name System (DNS) amplification attacks dropped four spots — from first to fifth — on our list of the most common type of single-vector attack in Q2.

Taking its place at the most commonly used single-vector attack in Q2 was Static Filtering — up 30% from Q1 and accounting for 24% of all single-vector attacks in the quarter.

Multi-vector mitigations

Top multi-vector mitigation type combinations

		QoQ
DNS, TCP SYN	13%	↓11%
DNS amplification, ICMP, TCP RST, TCP SYN/ACK amplification	10%	↑177%.
DNS, static filtering	6%	↓7%
DNS, TCP SYN, static filtering	5%	↓38%
UDP, static filtering	4%	↑20%
DNS amplification, TCP RST, TCP SYN/ACK amplification	3%	N.A.
Invalid packets, UDP	3%	N.A.
TCP SYN, static filtering	3%	↓25%
Invalid packets, static filtering	2%	N.A.
DNS amplification, ICMP, TCP RST, TCP SYN/ACK amplification, UDP	2%	↓47%.

DNS amplification combined with TCP SYN was the most commonly used vector combination, accounting for 13% of activity in Q2. This

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.

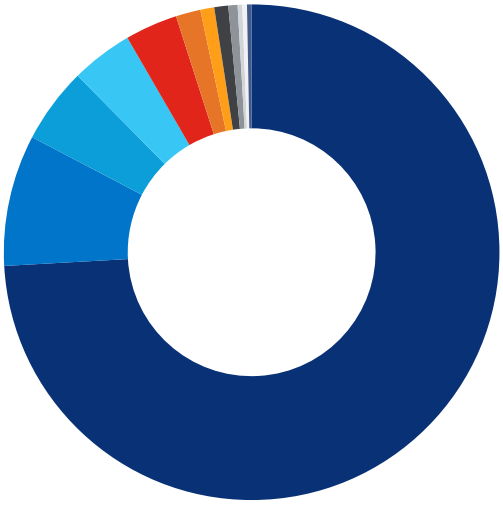
Learn more

was an 11% decrease compared to Q1, and a 37% decrease from Q2 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.

Additionally, in the Q1 report, we observed new multi-vector combinations including some that leveraged four and five different vectors (DNS Amplification, ICMP, TCP RST, TCP SYN/ACK Amplification and UDP amplification). That trend continued in Q2, and the second-most common multi-vector mitigation contained four different vectors: DNS Amplification, ICMP, TCP RST, and TCP SYN/ACK Amplification. This combination increased 177% since its debut in Q1 and accounted for 10% of the multi-vector attacks mitigated in Q2. As for the combination that contains five vectors, it declined 47% as the least commonly used combination, and accounted for just 2% of all multi-vector attacks that were mitigated in Q2.

Who is being attacked?

Largest 1,000 attacks by industry



Telecommunications	74%
Government	9%
Gaming	5%
Hosting	4%
Software & Technology	3%
Other	2%
Finance	1%
Insurance	1%
Healthcare	1%
Banking	0.3%
Education	0.3%
Media & Entertainment	0.3%
Utilities	0.2%
Business Services	0.2%
Manufacturing	0.2%
Retail & Distribution	0.1%

Of the 1,000 largest attacks Lumen mitigated in Q2, 95% targeted these top five verticals (in order): Telecommunications, Government, Gaming, Hosting, and Software and Technology. The telecommunications vertical continues to see large attack volumes due to the fact that a lot of companies obtain IP address space from telecom providers for their Internet service.

As we've reported in the past, a single government customer was attacked more than 2,600 times in Q2, representing 48% of all the attacks Lumen mitigated during the quarter. Most of these were small, short, single-vector attacks ranging from 5-10 minutes in duration. Of these, 37% came in the form of TCP SYN and 29% were DNS attacks.

Conversely, the largest attack Lumen mitigated in Q2 came from the telecommunications industry — 711 Gbps.

Telecommunications

- **74%** of the largest 1,000 attacks
- **1,378** total attacks
- Longest attack period duration: **8 days**
- Largest bandwidth attack: **711 Gbps**
- Largest packet-based attack: **202 Mpps**
- **60%** multi-vector attacks

Government

- **9%** of the largest 1,000 attacks
- **2,381** total attacks
- Longest attack period duration: **7 days**
- Largest bandwidth attack: **5.7 Gbps**
- Largest packet-based attack: **2.6 Mpps**
- **49%** multi-vector attacks

Gaming

- **5%** of the largest 1,000 attacks
- **82** total attacks
- Longest attack period duration: **5 days**
- Largest bandwidth attack: **415 Gbps**
- Largest packet-based attack: **36 Mpps**
- **60%** multi-vector attacks

Hosting

- **4%** of the largest 1,000 attacks
- **82** total attacks
- Longest attack period duration: **4 days**
- Largest bandwidth attack: **297 Gbps**
- Largest packet-based attack: **172 Mpps**
- **20%** multi-vector attacks

Software & Technology

- **3%** of the largest 1,000 attacks
- **492** total attacks
- Longest attack period duration: **5 days**
- Largest bandwidth attack: **95 Gbps**
- Largest packet-based attack: **23 Mpps**
- **22%** multi-vector attacks

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 number of customer complaints you must manage, and how much revenue is tied up in your websites and applications.

TESTING PARAMETERS

Industry:	Number of IT staff:	Annual online revenue:
Hosting	2 individual IT employees work on each security incident	$50M
Resulting IT helpdesk inquiries:	**Existing DDoS mitigation solutions:**	**Size of business in number of employees:**
5/hour	Yes	51-200

OUTCOMES

Yearly cost:	Number of DDoS attacks:	Average downtime:
$2,567,381	26	8 hours

With that in mind, let’s dive into a hypothetical use case: a mid-size Hosting company that earns $50 million in total online revenue. Their IT team is on the smaller side, with just two people dedicated to fixing security issues, including responding to DDoS attacks. During an attack they receive about five customer support calls per hour.

Based on data from our reports, we expect a company like this to be targeted 26 times annually, with an average downtime of eight hours per attack.

We anticipate the annual loss for this company is $2,567,381*. We found that revenue would be negatively impacted by $1,187,381, the cost impact from IT operations and customer support to be more than $28,000, and the negative brand impact to the organization to be $1,300,000. This would be for all 26 attacks combined, but ideally the organization would invest in DDoS mitigation services after the first incident. The bottom line is that 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

Rewind to Q1

In our previous report, we determined that a Retail & Distribution company that generated $152.7 million in online revenue is projected to have an annual financial loss of $2,946,021 from DDoS attacks. View the previous projection in more detail here.

LUMEN®

ThreatX API and Application Protection

ThreatX is a managed API and application protection provider 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 globe, ThreatX profiles attackers and blocks advanced risks to protect APIs and applications 24/7.

Learn more by viewing the ThreatX on Lumen Data Sheet

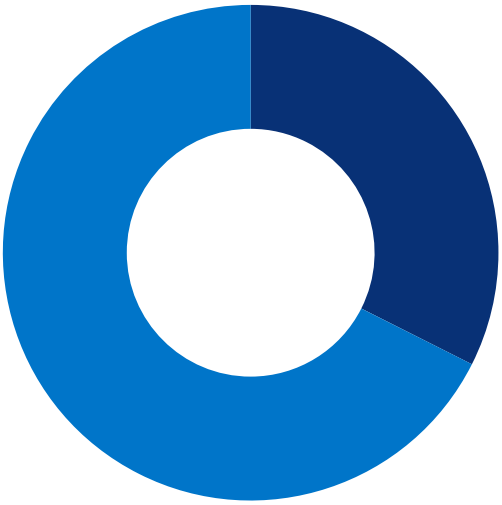
Application protection

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

	Q2 2023
Total requests	69 Billion
Total blocked requests	1.7 Billion
Blocked bot traffic	552 Million
Blocked due to other reasons	1.15 Billion



Percentage of blocked traffic that was malicious

Blocked bot traffic	32%
Blocked due to other reasons	68%

In the second quarter of 2023, ThreatX customers received a total of 69 billion requests to their applications. Of these, 1.7 billion requests were blocked in real-time.

In the previous report, the number of blocked requests was much higher. We mentioned that there may have been many reasons why there was such a large number of blocked requests, such as specific requirements set by ThreatX customers in order to access their applications. This may include **geofencing**, time parameters, and user device types (to name a few). However, in Q1 major outliers were removed from the data, resulting in the high percentage of total blocked attacks.

Geofencing

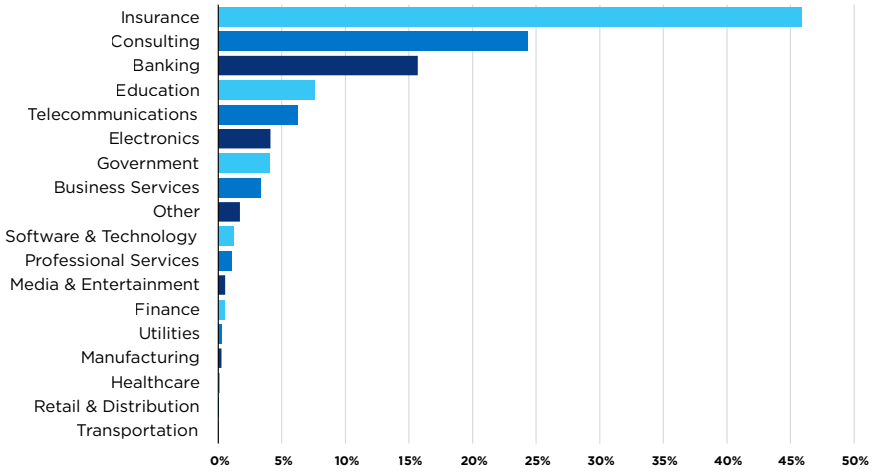
Geofencing limits an application's availability to users within specific locations determined by the application developers.

Within Q2, all ThreatX customers were included in the calculation of data.

Additionally, ThreatX customers blocked a total of 552 million requests due to bot traffic. This leaves 1.15 billion requests in Q2 that were blocked due to other reasons, which may include specific parameters set forth to access applications, or other potential threats attempting to access the applications.

Blocked API traffic by industry

% blocked API traffic



One major component of applications are APIs (application programming interfaces). APIs serve as the delivery mechanism for applications to share information and services with one another.

When we look at the breakdown of blocked API traffic by industry in Q2, the insurance sector had the highest percentage of blocked API traffic at 46%, followed by the consulting industry at 24% and banking at 16%.

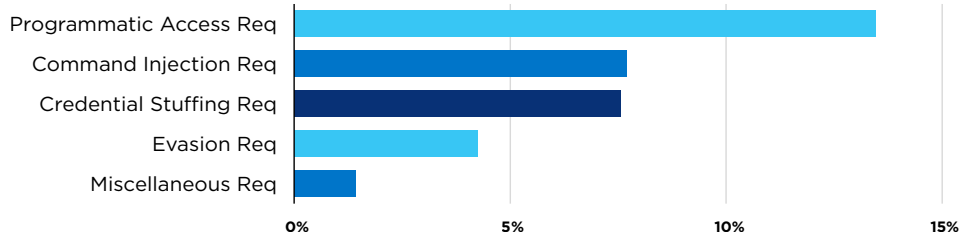
In Q2, ThreatX observed a significant increase in overall API traffic. According to ThreatX, there may be several reasons why we observed an increase in the overall API traffic quarter-over-quarter:

- **Increased adoption of APIs.** As more businesses adopt APIs, we can expect to see an increase in API traffic. This is because APIs make it easier for businesses to connect with each other and share data.
- **New API releases.** When new APIs are released, there is often a surge in traffic as businesses and developers experiment with the new features.
- **Marketing campaigns.** If a business runs a marketing campaign that promotes its APIs, we might see an increase in API traffic as more people learn about the APIs and start using them.
- **Security vulnerabilities.** If a security vulnerability is discovered in an API, we might see an increase in API traffic as cybercriminals try to exploit the vulnerability.
- **The growth of mobile apps.** Mobile apps are increasingly using APIs to access data and services.

- **The rise of cloud computing.** Cloud computing platforms often provide APIs that allow businesses to access and manage their cloud-based resources.
- **The Internet of Things (IoT).** IoT connects billions of devices to the internet, and many of these devices use APIs to communicate with each other.

ThreatX expects to see even more API traffic as these trends continue to grow.

Top 5 blocked application suspicions



Looking at the traffic ThreatX monitored for customers, some notable and suspicious activity occurred throughout Q2. This includes:

- The highest percentage of blocked traffic came from programmatic access accounting for 13.47% of the blocked traffic. Programmatic access is suspicious, automated access attempts against a web application.
- Next, command injection requests accounted for 7.7% of total blocked traffic.
- Credential stuffing requests accounted for 7.6% of total blocked requests in Q2.
- Evasion requests accounted for 4.3% of the total blocked requests observed in Q2.
- The fifth most observed attack included miscellaneous requests, which ThreatX defines as attempts to introduce known malicious code payloads into normal HTTP requests. Miscellaneous requests only accounted for 1.4% of all blocked traffic in Q2.

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 that 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, 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.

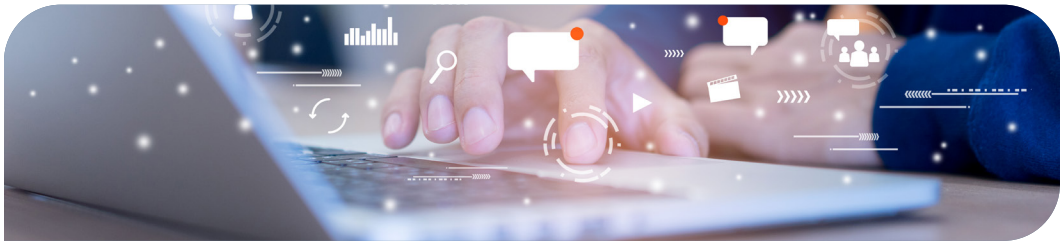
Final thoughts from Lumen

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 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.

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.



LUMEN®

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

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'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?

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.

LUMEN®

* 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 July 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 are from the timeframe of March 31, 2023, through July 1, 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.