REPORT

Lumen Quarterly DDoS Report

Q2 2021

LUMEN® TECHNOLOGIES

Introduction

This quarter we have seen some notable cyberattacks that have captured the public's attention. With consumers more aware of large-scale attacks, organizations have been under immense pressure to avoid being the next headline.

As businesses are working to secure a more remote and diverse ecosystem, their bad actor counterparts are not just looking to disrupt, they're trying to maximize the potential profits gained from an attack. Extortion has become a popular business model for criminal groups, and we've seen a growing reliance on ransom DDoS as an attack method.

Additionally, as an increasing number of businesses rely solely on digital interactions to engage with customers, their customer experiences and revenue streams are becoming more vulnerable. These are just a few contributing factors why Lumen mitigated 14% more DDoS attacks this quarter, and why we initiated a large number of emergency DDoS turns ups, mostly due to RDDoS.

In our Lumen Quarterly DDoS Report for Q2 2021, we examined intelligence from Black Lotus Labs® and data from the Lumen® DDoS Mitigation platform to develop our findings, which both reinforce and expand on these broader trends.

LUMEN® TECHNOLOGIES

Key findings for Q2 2021

IoT DDoS Botnets

- Lumen continues to track well-known IoT botnets like Gafgyt and Mirai. There was a 22% quarterly increase in unique C2s tracked across both families.
- The average lifespan of C2s nearly doubled from Q1.
- Of the nearly 1,150 DDoS C2s we tracked globally in Q2, the country hosting the most was the United States followed by Germany and the Netherlands.
- We observed nearly 300 C2s were issuing attack commands in Q2. The countries with the greatest number of C2s issuing commands were (in order): United States, The Netherlands and Germany.
- The country hosting the most DDoS botnet hosts was Brazil, going from ~12,000 in Q1 to more than 33,200 in Q2. Globally, Lumen tracked more than 150,200 infected hosts.

DDoS Attack Trends*

- The number of attacks we mitigated increased 14% compared to Q1, with a 10% increase in the number of sites attacked.
- In terms of bandwidth, the largest attack we scrubbed was 419 Gbps. In terms of packet rate, the largest attack we scrubbed was 132 Mpps. These represent quarterly increases of 56% and 408% respectively.
- The longest DDoS attack period we mitigated for an individual customer lasted 10 days.
- 69% of DDoS attack periods lasted less than one hour, and 12% of DDoS attack periods lasted 24 hours or more.
- Multi-vector mitigations represented 38% of all DDoS mitigations, with the most common using DNS query flood combined with a TCP SYN flood, which is consistent with Q1 findings.
- Static filtering, which is typically done on items such as port and protocol and provides an initial mitigation against attacks, was the most prevalent single-vector mitigation type. It was followed by UDP amplification.
- The top three verticals targeted in the 500 largest attacks in Q2 were: Telecom, Software and Technology, and Government.

IoT DDoS Botnets

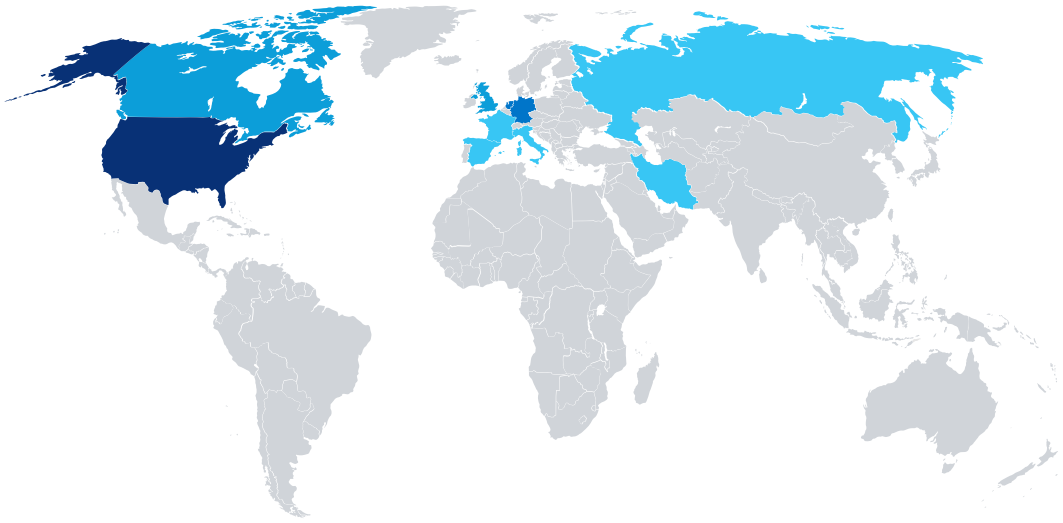
Family	Unique C2s tracked	Unique attack victims per family	Average lifespan of a C2 (in Days)
Gafgyt	505 ▲12% QoQ	1,528 ▼47% QoQ	32 ▲52% QoQ
Mirai	349 ▲40% QoQ	15,618 ▼38% QoQ	28 ▲180% QoQ

Black Lotus Labs, the threat intelligence arm of Lumen, has continued to monitor two predominate IoT DDoS families: Gafgyt and Mirai. We saw a 22% increase in total unique C2s tracked quarter over quarter, with the biggest increase seen with Mirai (40%). This was due to an increase in both activity and new variants. We also observed an increase in the average lifespan of the C2s, with Gafgyt increasing by 52% and Mirai increasing by 180%.

Global DDoS IoT Threats Tracked by Country

The following DDoS-specific heatmaps represent the top 10 countries by C2s tracked, C2s issuing attack commands, and botnet hosts. The data is based on Black Lotus Labs visibility and are broken down by threat type and suspected country of origin. Country of origin is determined by taking the IP address of each host and comparing it against a rich set of IP addresses to geographical mappings.

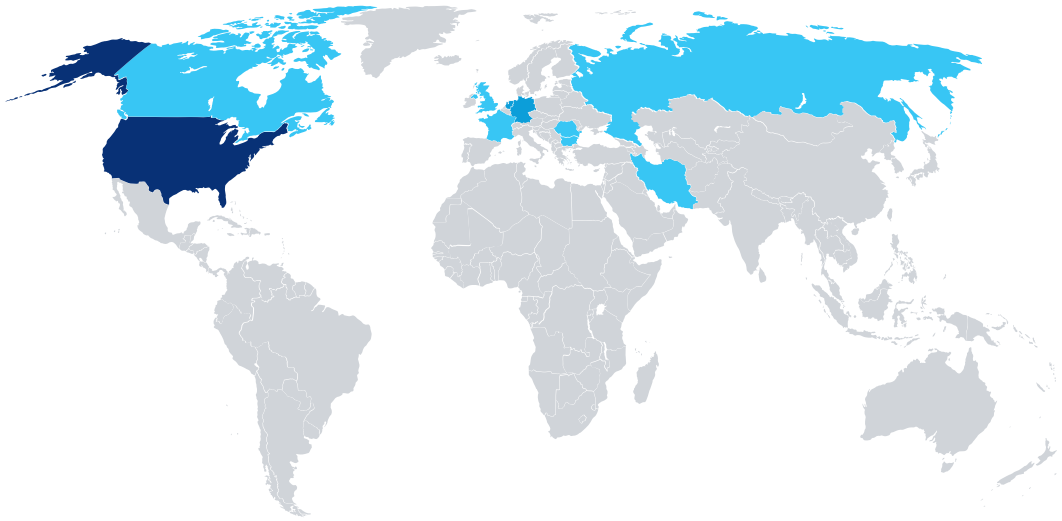
Top 10 Countries by C2s



Country Name	C2s	Population**	Per Capita (100,000)
United States	431	331,002,651	0.13
Germany	157	83,783,942	0.19
The Netherlands	152	17,134,872	0.89
Canada	54	37,742,154	0.14
United Kingdom	53	67,886,011	0.08
Spain	28	46,754,778	0.06
Italy	27	60,461,826	0.04
Russia	25	145,934,462	0.02
Iran	23	83,992,949	0.03
France	23	65,273,511	0.04

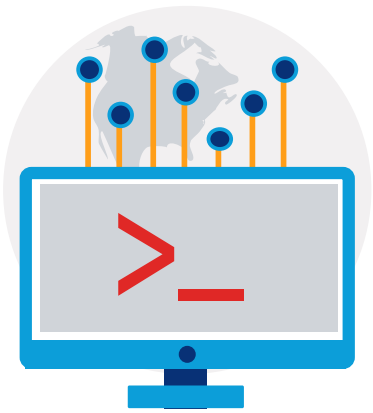
The country hosting the most DDoS C2s was the United States with a total of 431. Germany and the Netherlands followed in second and third place respectively, both hosting over 150 C2s each. The Netherlands also leads in number of C2s per capita (0.89), followed by Germany and Canada.

Top 10 Countries by C2s Issuing Attack Commands



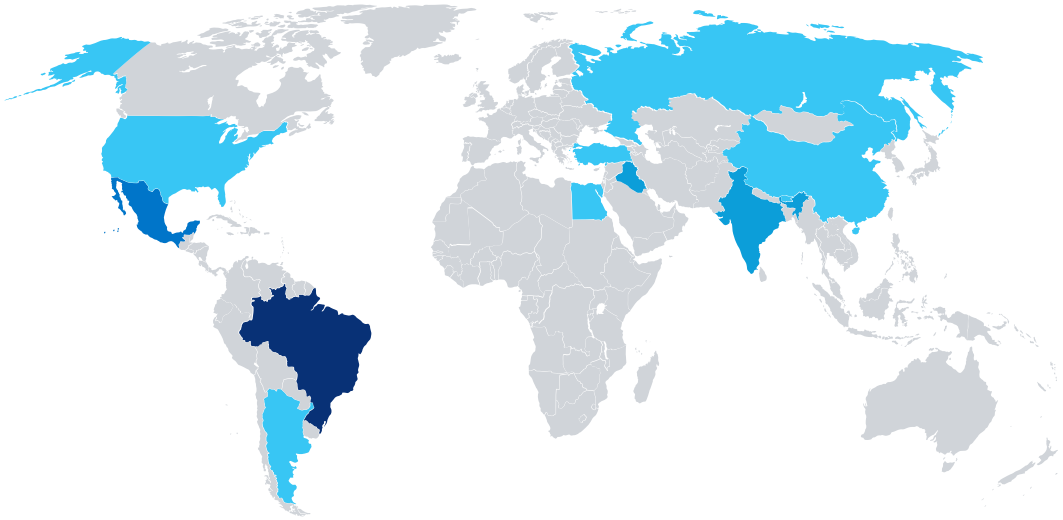
Country Name	C2s	Population**	Per Capita (100,000)
United States	131	331,002,651	0.04
The Netherlands	42	17,134,872	0.25
Germany	34	83,783,942	0.04
Canada	12	37,742,154	0.03
Romania	12	19,237,691	0.06
France	7	65,273,511	0.01
United Kingdom	6	67,886,011	0.01
Bulgaria	6	6,948,445	0.09
Russia	5	145,934,462	0.003
Iran	5	83,992,949	0.01

Overall, Black Lotus Labs saw the total number of C2s issuing attack commands decrease by 32%. However, the top three countries remain the same: United States, the Netherlands and Germany. Across the board we saw decreases quarter over quarter in our top 10 list apart from Bulgaria. which is new to the list this quarter. The countries with the most C2s issuing attack commands per capita were, in order, The Netherlands, Bulgaria and Romania.



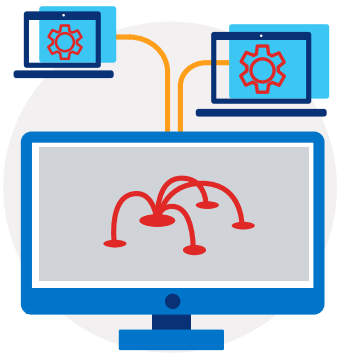
LUMEN® TECHNOLOGIES

Top 10 Countries by DDoS Botnet Hosts



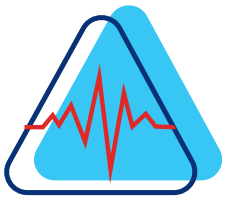
Country Name	Bots	Population**	Per Capita (100,000)
Brazil	33,269	212,559,417	15.65
Mexico	24,066	128,932,753	18.67
India	18,554	1,380,004,385	1.34
Iraq	10,683	40,222,493	26.56
Egypt	8,540	102,334,404	8.35
United States	6,997	331,002,651	2.11
Turkey	6,739	84,339,067	7.99
Argentina	6,082	45,195,774	13.46
Russia	4,052	145,934,462	2.78
China	3,835	1,439,323,776	0.27

Despite seeing an overall decrease of 10% in the bots we tracked, the top three countries hosting botnets saw huge increases quarter over quarter: Brazil: 173%; Mexico: 313%; and India: 70%. The United States dropped from its number one slot to sixth, decreasing by 83%. We also saw Turkey fall from the top three spot to the seventh. New entrants to the list were Russia and Argentina, while the United Kingdom and Lebanon fell off the list. The most botnet hosts per capita were, in order, Iraq, Mexico and Brazil.



Attack Size and Duration

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



	Dropped Bits/s	Dropped Pkts/s
Largest attack scrubbed	419 Gbps ▲56% QoQ	132 Mpps ▲408% QoQ

The two primary metrics for volumetric DDoS attacks are:

1. Attacks measured by bandwidth. These aim to disrupt service by flooding a circuit or application with traffic. This type of attack is measured by the bits per second.
2. Attacks measured by packet rate, which consume resources on network elements such as routers and other appliances.

The largest attacks of both types have increased quarter over quarter. The largest bandwidth attack we scrubbed in Q2 was 419 Gbps, which was a 56% increase from Q1. The largest high-packet throughput attack increased by more than 400%, going from 26 Mpps to 132 Mpps. Attacks of these sizes can easily disrupt most business operations when companies don't have a DDoS Mitigation solution.

While bad actors are continuing to launch large scale attacks, they are also relying on smaller and quicker attacks as their bread and butter. The average attack size that we scrubbed by bandwidth was 2 Gbps, and the average by packet was 416 Kpps.

Median Attack Duration

30 minutes

↑67% QoQ

Average Attack Duration

8 hours

6 minutes

↑11% QoQ

Longest Attack Duration

10 days

0 hours

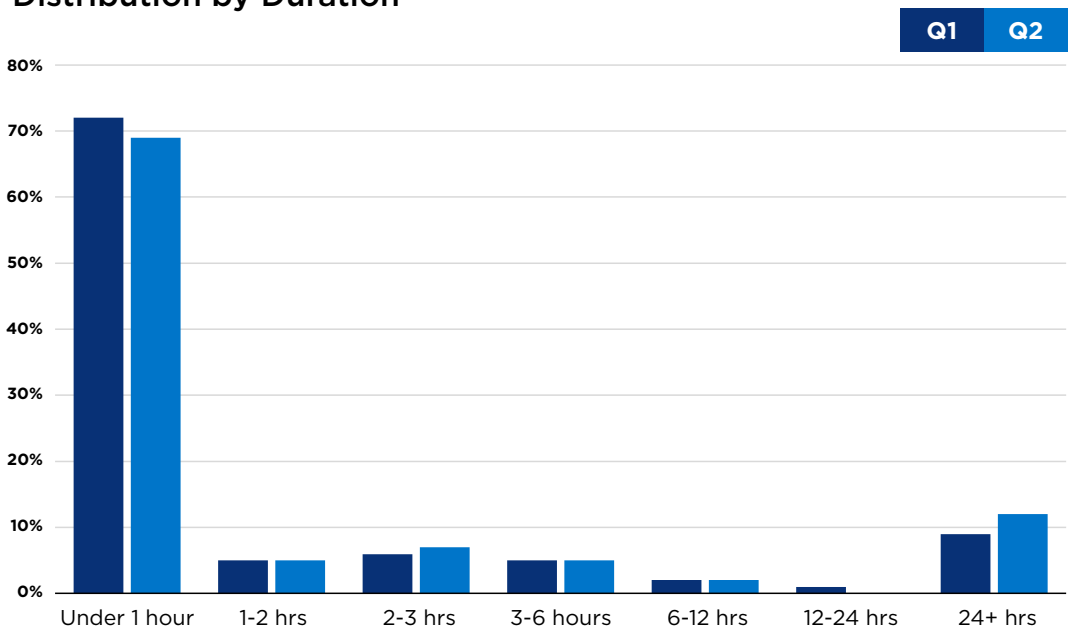
0 minutes

↓28% QoQ

Attack duration data suggests that the most frequent attacks are short in duration (<30 min). However, when attacks of duration longer than 30 minutes do occur, they tend to be significant campaigns with duration periods extended over multiple days and up to longer than a week. As an example, once a Ransom DDOS attack is executed, the attack can continue over multiple days or until the ransom is paid.

LUMEN® TECHNOLOGIES

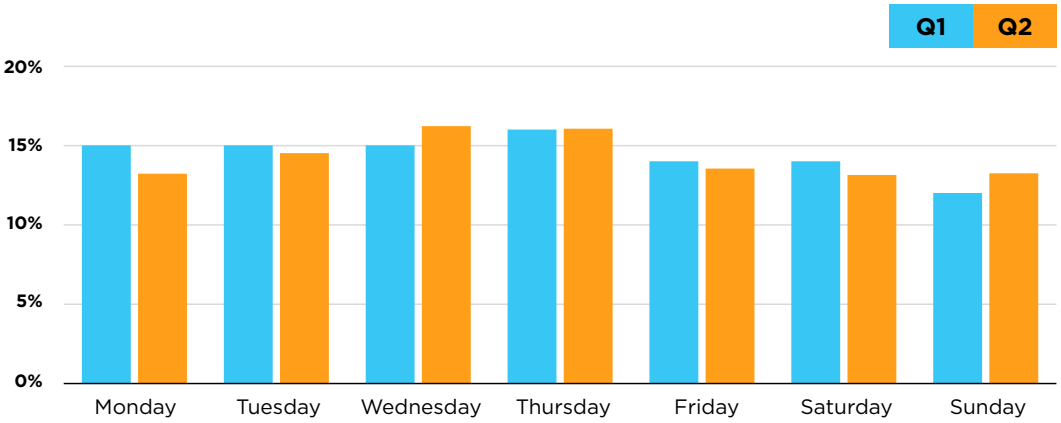
Distribution by Duration



Looking at the distribution by duration, Lumen found that attack periods lasting less than one hour decreased by 4% and accounted for 69% of all attacks. This is supported by the fact that the median attack period is around 30 minutes. We also saw an increase in 2–3-hour attacks, which increased 17% QoQ. The least frequent duration was 12-24 hours, accounting for no attacks this quarter.

Of all the attacks we mitigated, the percentage that lasted more than 24 hours increased from 9% in Q1 to 12% in Q2. We would like to note that this excludes Always-On mitigations which accounted for 19% of the total mitigated DDoS attacks; this is due to the fact that our system is constantly mitigating Always-On data.

Distribution by Day



Attacks by day of the week were in line with our first quarter findings,

with each day ranging from 13%-16% of all attacks. Midweek was slightly more likely to have an attack than the other days, while the weekends were only slightly less likely.

Attack Mitigation Types

Multi/Single-Vector Attacks

		QoQ
Multi-vector	38%	↓5%
Single-vector	62%	↑3%

The breakdown of single- and multi-vector attack mitigations was 38% and 62% respectively. This was a slight shift from Q1, which was a 40/60 split. Lumen expects these figures to fluctuate throughout the year.

Single-Vector Mitigations

Single-Vector Mitigation Type Breakdown

		QoQ
Static filtering	28%	↑38%
UDP amplification	22%	↑18%
Invalid packets	17%	↓15%
TCP SYN	15%	↓25%
DNS	8%	↓31%
Other volumetric	4%	↑30%
IP fragmentation	4%	↓29%
TCP RST	1%	-
HTTP	1%	-
SIP	1%	-
ICMP	1%	↓42%

Static filtering is typically done on items such as port and protocol. This vector type is also where our Black Lotus Labs threat feed mitigations are captured. It provides initial mitigation against attacks and was the most frequently used single-vector mitigation type, followed by UDP amplification, invalid packets and TCP SYN mitigation countermeasures. Invalid data packets include traffic with malformed data fields, as well as fragments that are incomplete, duplicate or too large. While they can be the result of network-related issues or faulty network sequencing, packet fragments are also a common characteristic of UDP amplification DDoS attacks.

UDP-based amplification attacks, which have always been prevalent, became a more common vector in Q2, with an 18% increase from Q1 to Q2. These attacks abuse application layer protocols and have proven to be powerful and capable of amplifying their potential impact. When launching an attack, actors manipulate the connectionless and stateless nature of UDP to spoof the source IP of a UDP request packet so that a victim receives unwanted UDP response packets from an unsuspecting intermediate service. Due to the size and volume of the response packets directed at the victim's IP, the victim's services become unavailable.

Multi-Vector Mitigations

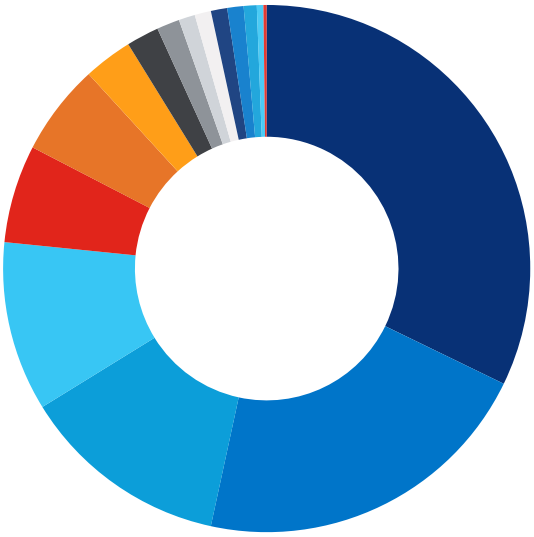
Top 10 Multi-Vector Mitigation Type Combinations

		QoQ
DNS, TCP SYN	10%	↓26%
Invalid packets, UDP	6%	↑38%
UDP, Static filtering	5%	↑166%
TCP SYN, UDP	5%	↑51%
Invalid packets, Static filtering	4%	↑103%
TCP SYN, Static filtering	4%	↑21%
DNS, TCP SYN, Static filtering	3%	↓17%
DNS, Static filtering	3%	↓18%
Invalid packets, UDP, Static filtering	3%	↓1%
DNS amplification, IP fragmentation	2%	↓64%

Multi-vector mitigations represented 38% of all DDoS mitigations, with the most common using a DNS query flood combined with TCP

SYN flood. We noticed a similar trend last quarter; however, the other combinations have shifted. In Q2, invalid packets with UDP amplification mitigations rose 38%, and UDP with static filtering mitigations more than doubled compared to Q1. DNS Amplification combined with IP Fragmentation saw the largest decrease. It was the second most common multi-vector mitigation in Q1, but dropped to tenth in Q2.

Largest 500 Attacks by Industry



Telecom	32%
Software & Technology	21%
Government	13%
Hosting	10%
Gaming	6%
Insurance	6%
Education	3%
Finance	2%
Media & Entertainment	1%
Utilities	1%
Banking	1%
Manufacturing	1%
Transport	1%
Business Services	1%
Unspecified	0.4%
Real Estate	0.2%

Of the 500 largest attacks, 83% targeted these top five verticals (in order): Telecommunications, Software and Technology, Government, Hosting, and Gaming. In addition, the Transportation vertical made the list since last quarter. Below are in-depth findings for the top five sectors:

Telecommunications

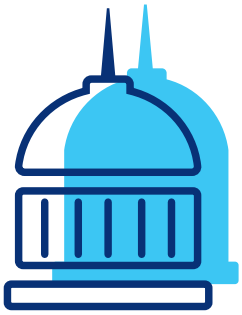
Telecom accounts for 32% of the 500 largest attacks we scrubbed — a decrease of 21% from Q1. Notably, most of these were against a single telecommunications company whose datacenter business was frequently attacked This sector experienced the single largest volumetric bandwidth attack that we scrubbed, which was 419 Gbps against another telecom. In addition, multi-vector attacks were more common than single-vector attacks against telecom companies, which is

opposite of our overarching observation that single-vector attacks were the most prevalent.

Sixty-seven percent of attack periods against telecom lasted less than an hour, which is 24% higher than the overall Q2 average. However, the longest attack period we mitigated was six days. When looking at the multi-vector mitigation combinations, the most frequent was IP fragmentation and other volumetric. This combination of countermeasures are used to mitigate UDP amplification attacks and indicate their prevalence.

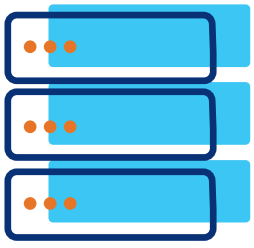
Software and Technology

Moving from third place to second, Software and Technology (S&T) saw a 41% increase in attacks from Q1 to Q2, which accounted for 21% of the largest attacks. The largest attack sizes were 233 Gbps (bandwidth) and 132 Mpps (packet-based). When it comes to timing, Thursdays were the most likely day for an attack (23%), and Sundays were the least likely (9%). Single-vector mitigations were the most frequent for this vertical (58%), which includes UDP amplification (28%), static filtering (27%) and invalid packets (25%) countermeasures. Bad actors targeting S&T companies mostly relied on quick attacks (44% lasted less than one hour). However, 43% of attacks were longer than 24 hours, which is 72% higher than our average.



Government

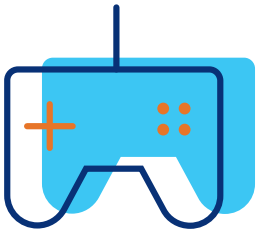
Of all attacks targeting this vertical, 78% lasted less than one hour. The next most common duration (7%) was 3-6 hours. When looking at mitigation type, 60% were single vector with the top three being TCP SYN (34%), DNS (19%) and static filtering (19%) countermeasures. Cybercriminals leveraged quick, common, and easy-to-mitigate attacks, meaning they were probably leveraging open-source code that's available on the dark-web.



Hosting

Attacks on the hosting vertical skyrocketed this quarter, going from 0.4% of the largest 500 attacks to 10% — a whopping 2,500% increase. These include attacks against the subscribers of hosting services. These attacks can affect all services in the hosting center, impacting other customers and the provider itself. The largest volumetric attacks were 264 Gbps (bandwidth) and 26 Mpps (packed based). This aligns with

the largest attack we saw in Q1 but was half the size of the largest attacks we scrubbed this quarter. When it came to duration, the attacks on hosting companies were more spread out than our quarterly averages and include the following durations: less than one hour (33%), 2-3 hours (24%) and more than 24 hours (22%). The hosting vertical did experience a 10-day attack period, which was the longest we mitigated. Single-vector mitigations were leveraged 19% more than the quarterly average (74% compared to 62% for Q2), with half of that being static filtering.



Gaming

The gaming vertical accounted for 6% of the largest 500 attacks we scrubbed this quarter, which aligns with Q1 findings. Attack size and duration were on the smaller end of the attacks we observed. The largest attack sizes were 24 Gbps for bandwidth and 2 Mpps for packet-based. Eighty-two percent of all attacks lasted less than one hour, and only 18% lasted longer than 24 hours (which is 25% below our quarterly average.) Attacks were more likely to occur on Thursdays (21%) and less likely to occur on Mondays (9%). Most mitigations were multi-vector (76%) with a reliance on the combination of CLDAP amplification, IP Fragmentation and UDP.

Ransom DDoS Can't Be Ignored

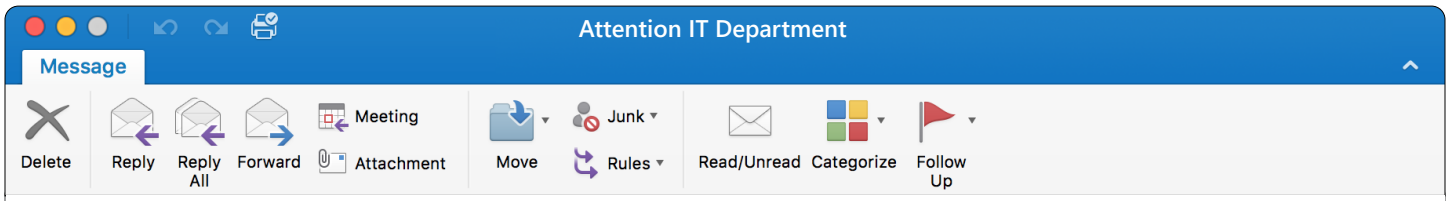
Ransomware is a popular choice for cybercriminals, but ransom DDoS (RDDoS) is also prevalent in today's threat landscape. According to the Lumen Global Security Operations Center (SOC) we have seen a number of our customers affected by RDDoS attacks.

Ransom DDoS is not an unusual tactic, but we have seen some new behavior that began in the fall of 2020 and continued in Q2 2021. To reinforce their threat, the actors almost always sent an immediate and small "test" attack to prove that they had the desire and the technical means to carry out the full-blown DDoS attack. In some cases, the groups taking responsibility claimed to be well-known threat actors including Fancy Bear, Lazarus Group, Armada Collective and have taken it upon themselves to create a new name by combining them to be Fancy Lazarus. The attacks launched were typically spoofed reflection attacks and, in general, were larger and more sustained than the average DDoS attack that we see.

What's the difference between Ransomware and Ransom DDoS?

Ransomware's primary means of attack is to encrypt an organization's systems and data. Hackers will only provide means to decrypt the data after a ransom is paid. In the case of ransom DDoS, bad actors threaten to launch a DDoS attack unless a ransom fee is paid, and failure to pay results in a service-impacting DDoS attack. Ransom DDoS is also referred to as Extortion DDoS.

During Q2 we had many new customers initiate emergency activation of DDoS mitigation service, and almost all of them were related to RDDoS. Below is a real extortion email that one of our customers received this quarter. The customer's name and other identifying information has been redacted for privacy.



Attention IT Department

FL

Fancy Lazarus

To: IT Department

We are the Fancy Lazarus and we have chosen [Customer name redacted] as target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days, on Wednesday next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from your [customer information redacted] block that will last for a cuple of hours. It will not

be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.) There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services. And worst of all you will lose Internet access in your offices too.

We will refrain from attacking your network for a small fee. The current fee is 2 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 4 BTC and will increase by 1 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [Bitcoin address redacted]

Once you have paid we will automatically get informed that it was your payment.

Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied.

As of the drafting of this report 1 bitcoin is equal to around $39,500 USD, which means that in the extortion letter above attackers were asking for $79,024 as the current fee and $158,047 USD once the attack began.***

LUMEN® TECHNOLOGIES

Key Takeaways

Spotting a DDoS attack might seem easy, but a wide range of attack types and tactics make it deceptively difficult in many cases. Attackers aren't going to give you a heads up that they're going to make a move, and victims are immediately put on the spot to defend themselves. Some defensive measures include:

- Monitor the level of incoming network traffic and look for unexpected spikes that deviate from your baselines.
- Watch the number of requests sent to a protected IP address space. Set a threshold to alert you when an IP receives more than a set number of requests in each period. Consult baselines when setting thresholds.
- If an application is sluggish or unresponsive — perhaps even giving you a 503 error — you might be experiencing a "low and slow" attack. You can set your server operating system to alert you when those HTTP responses start appearing.
- Be prepared for an attack — it is not a matter of if, but when. You must have an effective plan in place with a DDoS mitigation provider.

These are just a few potential symptoms of an ongoing DDoS attack. You should explore your logs and data to verify.

With the increase in size, complexity and types of DDoS attacks, organizations cannot risk their income, customer experience or reputation. A good DDoS mitigation solution is basic cybersecurity hygiene not unlike dental hygiene. If you don't brush your teeth, it's not a matter of *if* you get a cavity — it's a matter of *when* and how *painful* it's going to be.

Throughout this report we have discussed Q1 and Q2 findings, and while it's important to review the first half of 2021, we are continually learning about emerging threats. Be on the lookout for our Q3 Quarterly DDoS Report in November to read about the latest threat landscape.

Guidance for Network Defenders

Network defenders should look for a DDoS mitigation provider that can offer:

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

How Lumen Can Help You Today

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

Learn more about Lumen DDoS Mitigation

If you're interested, read our Q1 Quarterly DDoS Report

LUMEN® TECHNOLOGIES

Methodology

Data in this report is from the timeframe of April 1, 2021, through June 30, 2021.

Scrubbed attacks are defined as either:

- Incidents flagged by high-level alerts mitigated by the platform, or
- Periods in running mitigations where individual countermeasures are dropping traffic, or
- Events where dropped traffic exceed passed traffic.

Attack vectors or mitigation types are identified either by countermeasures dropping traffic, or misuse types flagged in our flow-based monitoring.

Peaks in the data may be attenuated by how rates are averaged over various time increments.

Data from our Always-On customers is aggregated in increments of minutes, hours or days according to the length of time a mitigation runs. If a mitigation runs long enough that the resolution time reaches a length of one day, and if there are multiple sequential days of attack, then it is counted as a single multi-day period of attack.

Endnotes

* We continue to refine our algorithms. Numbers for Q1 2021 used for quarter-over-quarter comparisons were recalculated using the same methods used for Q2 2021 and vary slightly from the published Lumen DDoS Q1 Report.

** Source: Worldometer (www.worldometers.info)

*** Data provided by Morningstar for Currency and Coinbase for Cryptocurrency.

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

LUMEN® TECHNOLOGIES