REPORT

Lumen Quarterly DDoS Report

Q1 2021

LUMEN® TECHNOLOGIES

Introduction

The last year was another active one for the DDoS attack space. The common themes of recent years — increased complexity, frequency and scale — continued to drive the space with actors shifting and adopting tactics, techniques and procedures (TTPs), including multi-vector and mixed application layer attacks and diversifying their victim pools to maximize impact and/or profit.

As an industry, we saw one of the largest attacks on record in the first quarter of 2020 with 2.3 Tbps*, followed by a slate of ransom DDoS (RDDoS) over the summer and fall targeting finance and healthcare, among other industries.

In addition, the continued evolution of IoT botnets capable of waging DDoS attacks, coupled with widely accessible botnet source code and DDoS-for-rent infrastructure have reduced the minimum competencies required to launch attacks, further expanding the potential actor pool.

Against this backdrop, today's enterprises are challenged with a growing dependence on revenue from digital applications to serve and engage customers, an unprecedented uptick in traffic spurred by widespread reliance on digital services and the pressure to satisfy end user expectations for seamless application delivery and always-on performance.

In our Lumen Quarterly DDoS Report for Q1 2021, we share our view of the DDoS landscape with findings that both reinforce and expand on these broader trends, with a look into DDoS threats based on intelligence from Black Lotus Labs®, as well as attack trends from the Lumen® DDoS Mitigation Service platform.

Key findings for Q1 2021

IoT DDoS Botnets

- Well-known IoT botnets like Gafgyt and Mirai remain serious DDoS threats, with 700 active C2s attacking 28,000 unique victims combined.
- Out of a total of nearly 3,000 DDoS C2s we tracked globally in Q1, the country hosting the most C2s is Serbia, followed by the United States and China.
- Of the more than 400 C2s globally that we observed issuing attack commands, the country with the greatest number was the United States, followed by The Netherlands and Germany.
- Of the more than 160,000 global DDoS botnet hosts we tracked, the greatest number are located in the United States, with nearly 42,000 bots.

DDoS Attack Trends

- The largest attack measured by bandwidth we scrubbed was 268 Gbps and the largest attack measured by packet rate we scrubbed was 26 Mpps.
- The longest DDoS attack period we mitigated for an individual customer lasted almost two weeks.
- Nearly 60% of DDoS attack periods lasted less than one hour, but nearly 20% of DDoS attack periods lasted more than 24 hours.
- Multi-vector mitigations represented 41% of all DDoS mitigations, with the most common using a DNS query flood combined with a TCP SYN flood.
- Static filtering, typically done on items such as port and protocol, provide an initial mitigation against attacks, and was the most prevalent single vector mitigation type, followed by invalid packets, UDP amplification and TCP SYN.
- The top three verticals targeted in the 500 largest attacks in 1Q21 were: Finance, Software & Technology and Government.

IoT DDoS Botnets

Family	Unique C2s tracked	Unique attack victims per family	Average lifespan of a C2 (in Days)
Gafgyt	451	2,870	21
Mirai	249	25,240	10

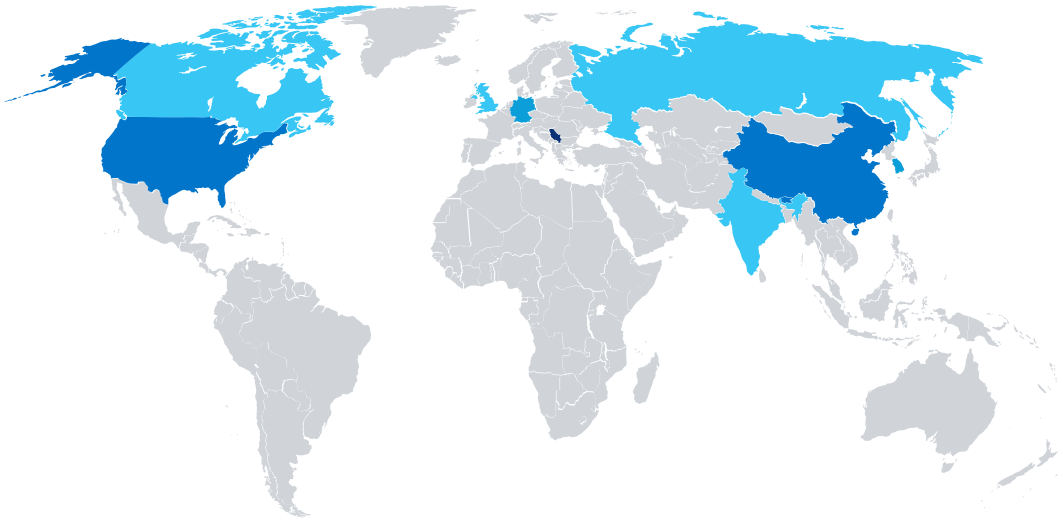
As in previous reports, Black Lotus Labs continues to monitor two of the most predominate IoT DDoS families, Gafgyt and Mirai. Notably, despite the number of Mirai C2s totaling a little more than half those of Gafgyt in the first quarter, and despite having a much shorter average lifespan, Black Lotus Labs has identified roughly 10 times as many unique Mirai attack victims as those of Gafgyt.

LUMEN® TECHNOLOGIES

Global DDoS Threats Tracked by Country

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

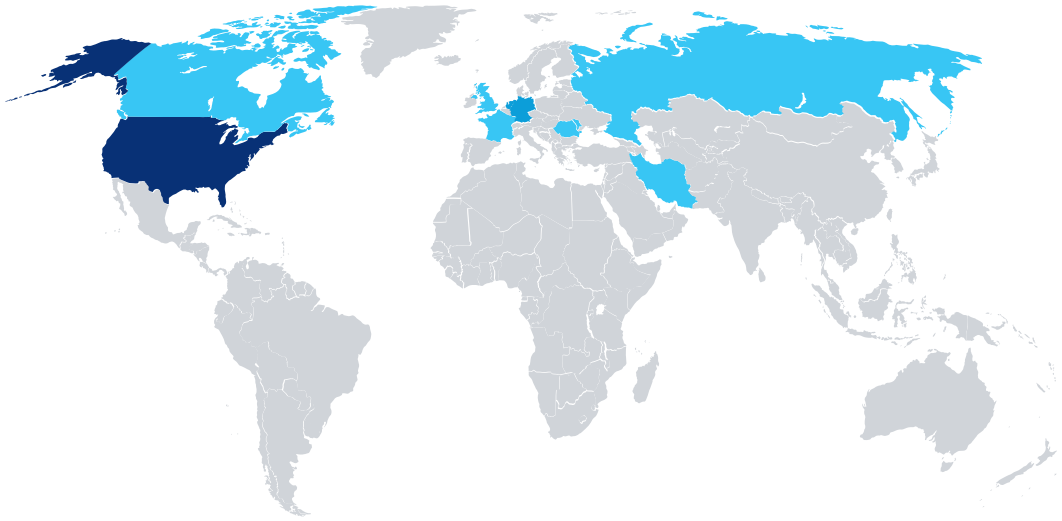
Top 10 Countries by C2s



Country Name	C2s	Population**	Per Capita (100,000)
Serbia	1,260	8,737,371	14.42
United States	380	331,002,651	0.11
China	373	1,439,323,776	0.03
South Korea	166	51,269,185	0.32
Germany	138	83,783,942	0.16
The Netherlands	132	17,134,872	0.77
Canada	53	37,742,154	0.14
Russia	41	145,934,462	0.03
United Kingdom	38	67,886,011	0.06
India	36	1,380,004,385	0.003

The country hosting the most DDoS C2s is Serbia with a total of 1,260, followed by the United States and China with 380 C2s and 373 C2s, respectively. Serbia also has the highest number of C2s per capita with more than 14 C2s per 100,000 people, followed distantly by The Netherlands and South Korea.

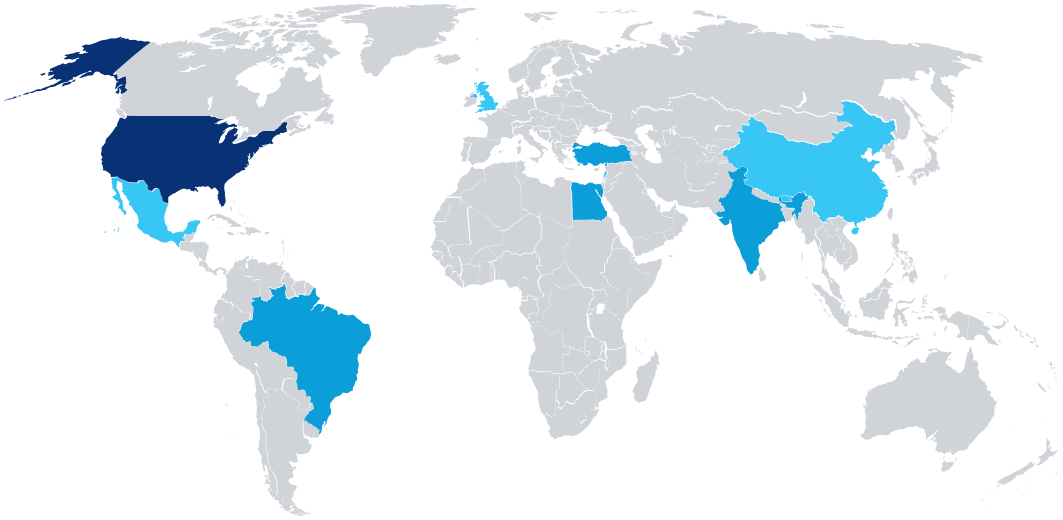
Top 10 Countries by C2s Issuing Attack Commands



Country Name	Number of C2s	Population**	Per Capita (100,000)
United States	163	331,002,651	0.05
The Netherlands	73	17,134,872	0.43
Germany	70	83,783,942	0.08
Canada	15	37,742,154	0.04
United Kingdom	14	67,886,011	0.02
France	13	65,273,511	0.02
Romania	13	19,237,691	0.07
Russia	12	145,934,462	0.01
Iran	8	83,992,949	0.01
Moldova	8	4,033,963	0.20

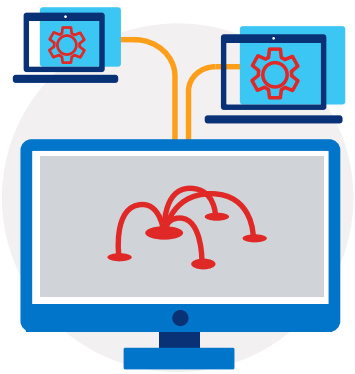
The country with the largest number of tracked C2s observed issuing attack commands in this timeframe is the United States, followed by The Netherlands and Germany. The Netherlands had the greatest number of C2s per capita, followed by Moldova and Germany.

Top 10 Countries by DDoS Botnet Hosts

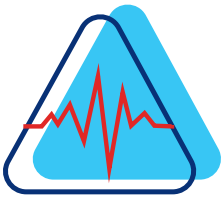


Country Name	Number of Bots	Population**	Per Capita (100,000)
United States	41,752	331,002,651	13
Iraq	23,647	40,222,493	59
Turkey	12,921	84,339,067	15
Brazil	12,196	212,559,417	6
Egypt	11,009	102,334,404	11
India	10,939	1,380,004,385	1
China	7,371	1,439,323,776	1
Mexico	5,821	128,932,753	5
Lebanon	3,612	6,825,445	53
United Kingdom	3,168	67,886,011	5

Of the more than 166,000 DDoS botnet hosts we tracked in the first quarter, the greatest number of hosts are located in the United States, with nearly 42,000 bots. On a per capita basis, the most DDoS bots per 100,000 people are located in Iraq and Lebanon, with 59 and 53, respectively.



Attack Size and Duration



	Dropped Bits/s	Dropped Pkts/s
Largest attack scrubbed	268 Gbps	26 Mpps

Lumen absorbs 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 the Lumen network.

Lumen analyzes and mitigates two primary types of volumetric DDoS attacks: those measured by bandwidth which disrupt service through flooding a circuit or application with traffic measured in bits per second, and those measured by packet rate which can also tie up specific network resources such as routers or other appliances in the network and are measured in packets per second. Attack sizes in this report convey the largest attacks scrubbed by Lumen global DDoS scrubbing infrastructure, rather than the largest attacks observed entering the Lumen network.

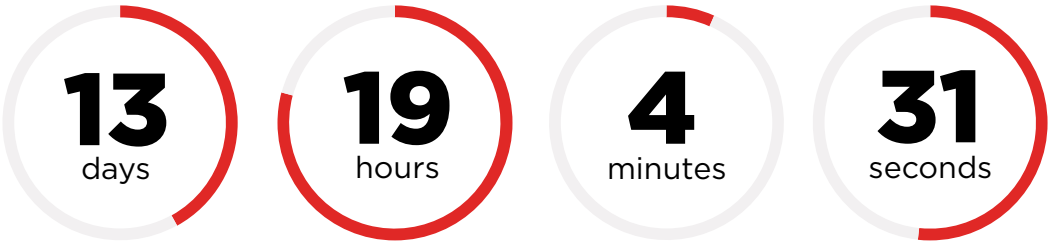
The largest Q1 attack measured by bandwidth we scrubbed was 268 Gbps. Many businesses today do not have the capacity to withstand a 250+ Gbps attack, which is the equivalent of more than 50 million plain text emails all being received at the same time.

The largest high-packet throughput attack we scrubbed for the quarter was 26 Mpps, which equates to 62 10 GigE ports based on an average packet size of 300 bytes, which could easily overwhelm router resources such as CPU, forwarding, memory and other functions.

Median Attack Duration

Average Attack Duration

Longest Attack Duration

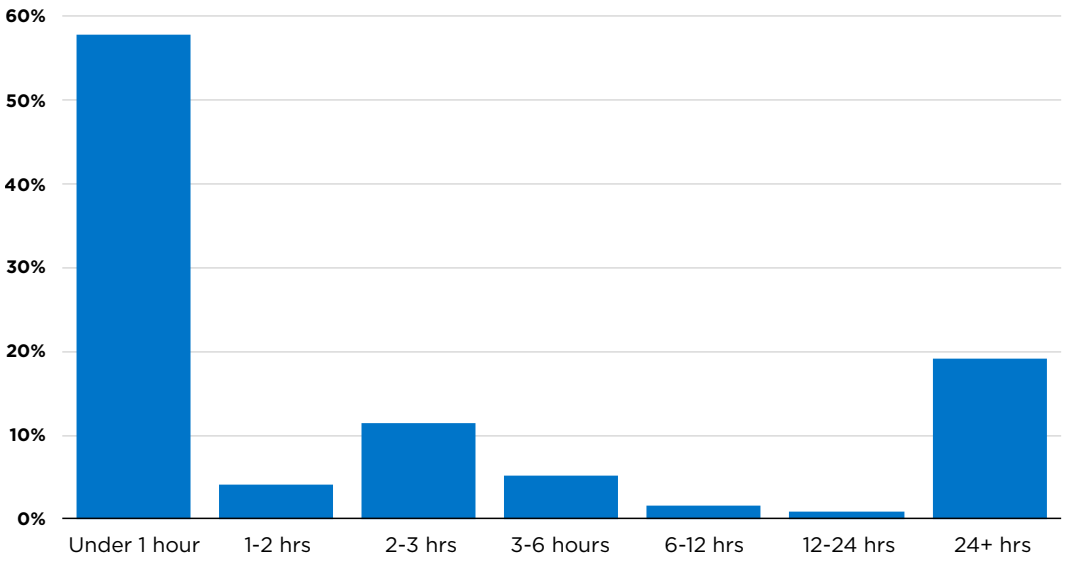


While the median attack period duration was just under 26 minutes, the longest attack period we observed lasted nearly two weeks. On average, DDoS attack periods in the first quarter lasted nearly seven hours.

Nearly 60% of DDoS attack periods lasted less than one hour, but nearly 20% of DDoS attack periods lasted more than 24 hours.

LUMEN® TECHNOLOGIES

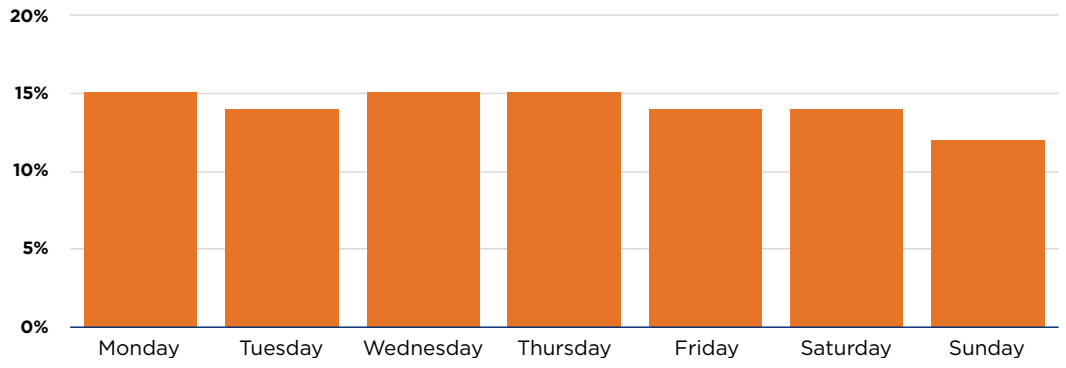
Distribution by Duration



Looking at the distribution by duration, we found that nearly 60% of DDoS attack periods lasted less than one hour, but nearly 20% of DDoS attack periods lasted more than 24 hours. Interestingly, the next greatest percentage of DDoS attack period duration was in the 2 to 3-hour timeframe, with 11%.

While it's not surprising that the majority of attacks would be less than an hour, given DDoS mitigation service provider SLAs in the 10-15 minute range, it is notable to see such a sizable percentage of attack periods lasting more than 24 hours. For buyers that are sensitive to the SLAs, always-on mitigation where the traffic is sent through scrubbers all the time may be the appropriate choice.

Distribution by Day



We also investigated whether DDoS attacks were more likely to occur on certain days than others, but found distribution across days of week

was fairly pretty consistent, with 14-15% of attacks falling on each day Monday through Saturday, and then a slight drop off on Sundays with 12% of attacks. Even DDoS operators need a break it seems.

Attack Mitigation Types

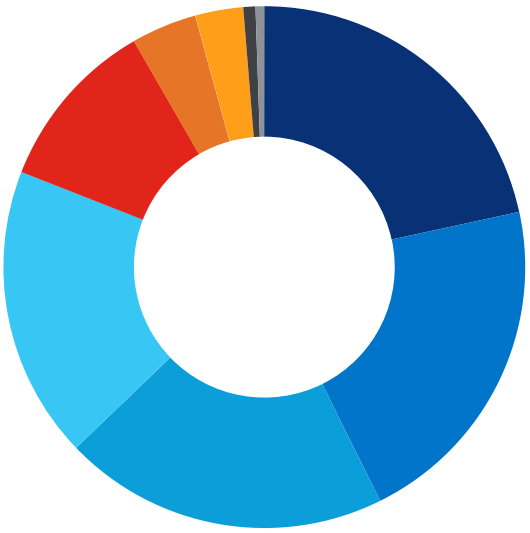
Multi/Single-Vector Attacks

Multi-vector	41%
Single-vector	59%

The breakdown of single to multi-vector attacks is roughly 60% to 40%, respectively. In recent years, the mix of single to multi-vector has fluctuated, with some in the industry believing multi-vector attacks would far surpass single vector attacks. However, given the broad availability of DDoS botnet source code and the relative ease with which DDoS attack infrastructure can be rented via the dark web — which can extend DDoS attack capabilities to less sophisticated actors — it's not surprising to see a sizable portion of attacks being waged across a single vector. In addition, more sophisticated actors may also leverage single vector attacks to launch DDoS for the purpose of distracting the victim from their real goal, such as data exfiltration.

Single-Vector Mitigations

Single-Vector Mitigation Type Breakdown



Static filtering	21%
Invalid packets	21%
UDP amplification	20%
TCP SYN	18%
DNS	11%
IP fragmentation	4%
Other volumetric	3%
ICMP	1%
TCP SYN/ACK reflection	1%

Static filtering, typically done on items such as port and protocol, provides an initial mitigation against attacks, and was the most prevalent single vector mitigation type, followed by invalid packets, UDP amplification and TCP SYN. Invalid packets includes traffic with malformed data fields, as well as fragments that are incomplete, duplicate or too large. While they can be the result of a network bug or faulty network sequencing, they are also a common characteristic of DDoS attacks.

UDP-based amplification attacks are a common vector targeting application layer protocols and have proven to be a powerful vector capable of greatly amplifying their potential impact. In these attacks, actors manipulate the connectionless and stateless nature of User Datagram Protocol to spoof the source IP of a UDP request packet so that a victim receives unwanted UDP response packets from an unsuspecting intermediate server. Because UDP responses to certain queries or services can be much larger than request packet sizes, the victim IP can quickly become overwhelmed.

During UDP amplification DDoS attacks, often the responses generated by the servers being used to amplify messages must respond in fragments due to the size of the response. The increased processing load which this causes on routers handling massive floods can lead to lost or malformed fragments. This causes UDP amplification attacks to exist within both the UDP amplification area as well as the invalid area. In addition, for many of our customers, we utilize static filtering to completely block some of this traffic, making UDP amplification have an impact across many mitigations and demonstrating how common it is as an attack vector.

TCP SYN attacks exploit TCP's three-way handshake by never responding with the required acknowledge packet, leaving a server to hold potentially tens or hundreds of thousands of open connections, causing it to exhaust either socket space, ephemeral port space, memory space, and the like.

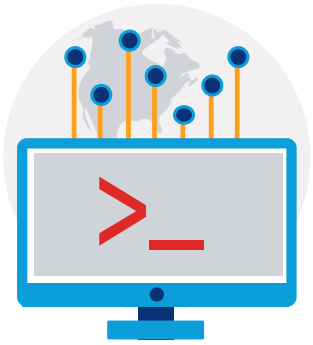
Multi-Vector Mitigations

Top 10 Multi-Vector Mitigation Type Combinations

DNS, TCP SYN	12%
DNS amplification, IP fragmentation	4%
TCP SYN, UDP	4%
DNS, TCP SYN, static filtering	4%
Invalid packets, UDP	3%
DNS, static filtering	3%
IP fragmentation, total traffic, UDP	3%
Invalid packets, static filtering	3%
TCP SYN, static filtering	3%
Invalid packets, UDP, static filtering	2%

Multi-vector mitigations represented 41% of all DDoS mitigations, with the most common using a DNS query flood combined with a TCP SYN flood. DNS-based DDoS attacks here refer to DNS floods, where attackers seek to disrupt Domain Name System servers to prevent DNS resolution of a given domain. These attacks often randomize questions so that DNS' natural caching mechanisms will not protect the server.

Other repeated combinations we found, all occurring at roughly the same frequency, include DNS amplification and IP fragmentation, TCP SYN and UDP, and invalid packets and UDP. These combinations reflect standard vectors used to wage DDoS attacks, but combined in various ways for greater impact.



BLACK LOTUS LABS®

Tracking UDP Reflectors for a Safer Internet

In recent years, Distributed Denial of Service (DDoS) events have become an ever-present threat, featuring attack traffic pushing to levels measured in terabits per second (Tbps). One of the key tools in the hands of cybercriminals seeking to increase the bandwidth of their attacks is UDP-based reflection.

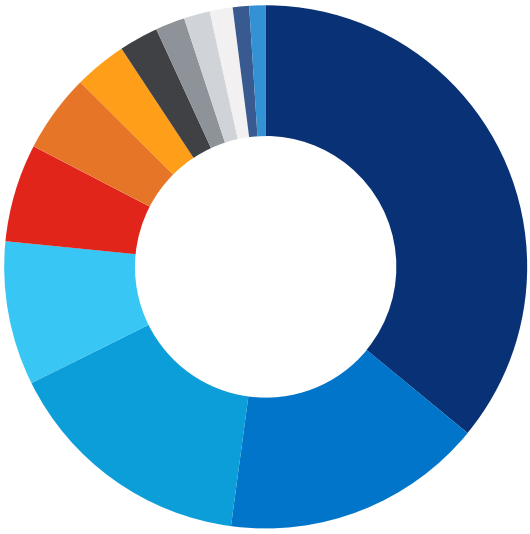
For example, the 2018 DDoS attack on GitHub made use of an application layer service called Memcached to direct, at peak, 1.35 Tbps of reflected UDP traffic at GitHub's servers. In 2020, the industry learned about a 2017 DDoS attack that used a bundle of UDP services as reflectors (CLDAP, DNS, and SMTP) to achieve wire rates of up to 2.5 Tbps.

At Black Lotus Labs, we leverage visibility from our global network to identify services potentially being manipulated to launch attacks, such as Memcached instances, CLDAP and DNS, and then work to confirm whether they are open to use as reflectors. Based on our data from the first quarter of 2021, we see each of these services being actively used to launch significant DDoS attacks today.

Read our blog, Tracking UDP Reflectors for a Safer Internet, to learn more.

LUMEN® TECHNOLOGIES

Largest 500 Attacks by Industry



Finance	36%
Software & Technology	16%
Government	15%
Telecomm	9%
Gaming	6%
Education	5%
Other verticals	3%
Utilities	2%
Retail and Distribution	2%
Consulting	2%
Business Services	1%
Not for Profit	1%
Healthcare	1%

Of the 500 largest attacks, two-thirds targeted just three verticals (in order): Finance, Software & Technology and Government. The finance vertical experienced the most volumetric attacks, with 36% of the 500 largest attacks. Software & Technology experienced 16% of the largest attacks, and the Government sector, which includes state, local and federal, experienced 15%. Finance has long been a target of DDoS attacks, but this distribution shows that no vertical is spared in today's threat landscape.

The top three verticals targeted in the 500 largest attacks in 1Q21 were Finance, Software & Technology and Government.

LUMEN® TECHNOLOGIES

Key Takeaways

For next-gen applications and modern workloads — the lifeblood of the digital economy — expectations are high. It's all about user experience, which hinges on availability, performance and security.

As the dependency on applications to generate revenue deepens, many organizations are realizing they can no longer risk foregoing essential DDoS defenses. Organizations must protect critical web-facing assets and applications from increasingly complex attacks — all with limited in-house talent, an expanding attack surface and an inherent need to mitigate large attacks in the cloud or network.

They need a service provider with global reach and highly scalable mitigation capacity that offers carrier agnostic protection against multi-vector and mixed application layer attacks, with advanced features like always-on service and automated threat detection and response to help stop attacks before they hit the customer network.

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
- Global footprint for reduced latency when routing traffic for scrubbing
- Flexibility and advanced features to protect modern web 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 the data center to the cloud

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

Learn more about Lumen DDoS Mitigation Service

LUMEN® TECHNOLOGIES

Methodology

Data in this report is from the timeframe of January 1, 2021 through March 31, 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 by either countermeasures dropping traffic or misuse types flagged in our flow-based monitoring.

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

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

Endnotes

* Source: https://www.tripwire.com/state-of-security/security-data-protection/amazon-web-services-mitigated-a-2-3-tbps-ddos-attack/

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

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

LUMEN® TECHNOLOGIES