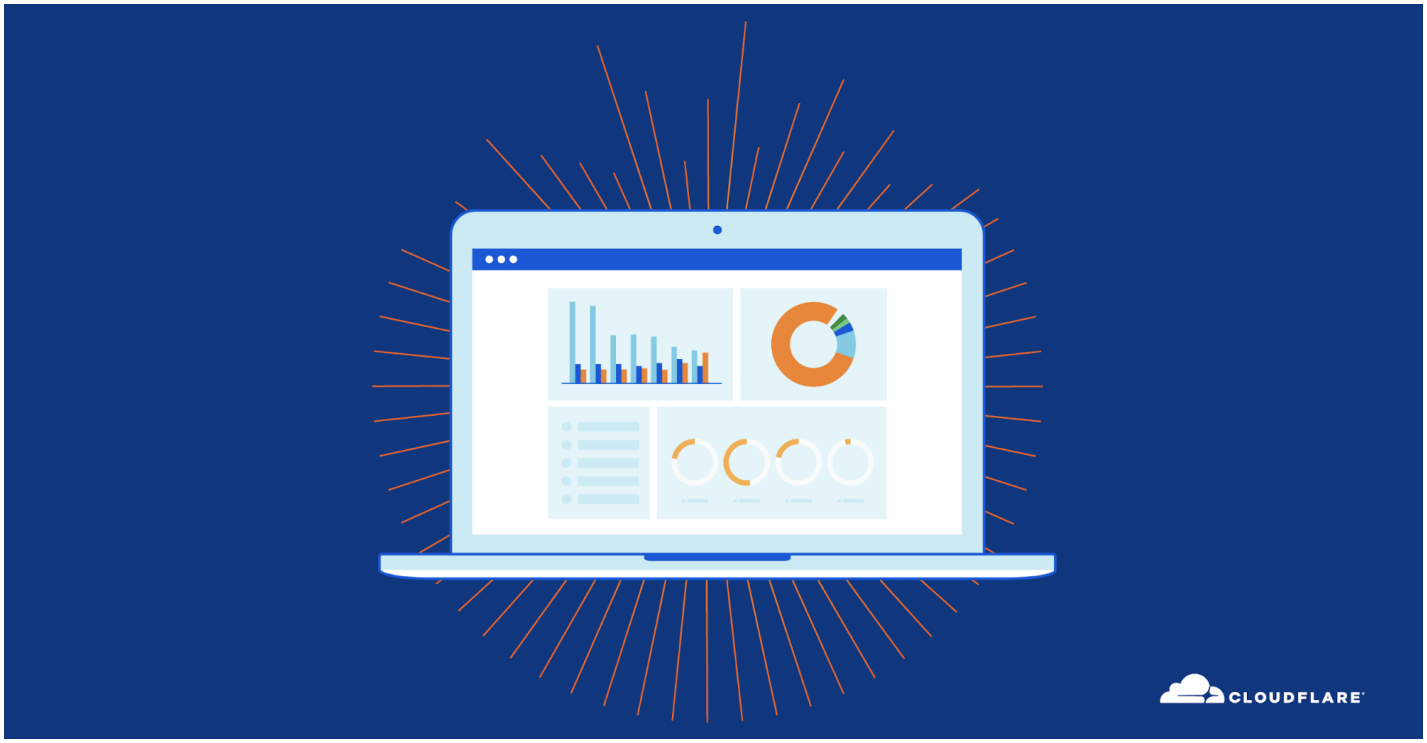
DDoS attack trends for 2021 Q1

04/19/2021

 Vivek Ganti  Omer Yoachimik

10 min read



Last week was Developer Week at Cloudflare. During that week, our teams released a bunch of cool new products, including a bunch of improvements to Workers. And it's not just our customers that love deploying apps with Workers, but also our engineering teams. Workers is also what powers our Internet traffic and attack trends on Cloudflare Radar. Today, along with this deep-dive analysis blog, we're excited to announce the new Radar DDoS Report page, our first fully automated data notebook built on top of Jupyter, Clickhouse, and Workers.

Last month, we introduced our autonomous edge DDoS (Distributed Denial of Service) protection system and explained how it is able to drop attacks at wire speed without impacting performance. It runs in our networks' edge, analyzes

traffic asynchronously to avoid impacting performance, and pushes mitigation rules in-line immediately once attacks are detected. All of this is done autonomously, i.e., without requiring centralized consensus.

Today, we'd like to share the latest DDoS insights and trends that are based on attacks that our system mitigated during the first quarter of 2021. When we analyze attacks, we calculate the "DDoS activity" rate, which is the percent of attack traffic out of the total traffic (attack + clean). This allows us to normalize the data points and avoid biases towards, for example, a data center that sees more traffic and therefore also more attacks.

Highlights

Application-layer DDoS attacks

- In 2021 Q1, the country with the highest percentage of HTTP attack traffic was China. This was followed by the United States, Malaysia, and India.
- The telecommunication industry was the most attacked in Q1, followed by Consumer Services, Security and Investigations, Internet, and Cryptocurrency.
- The most attacked Internet properties were of companies based in China, the US, and Morocco.

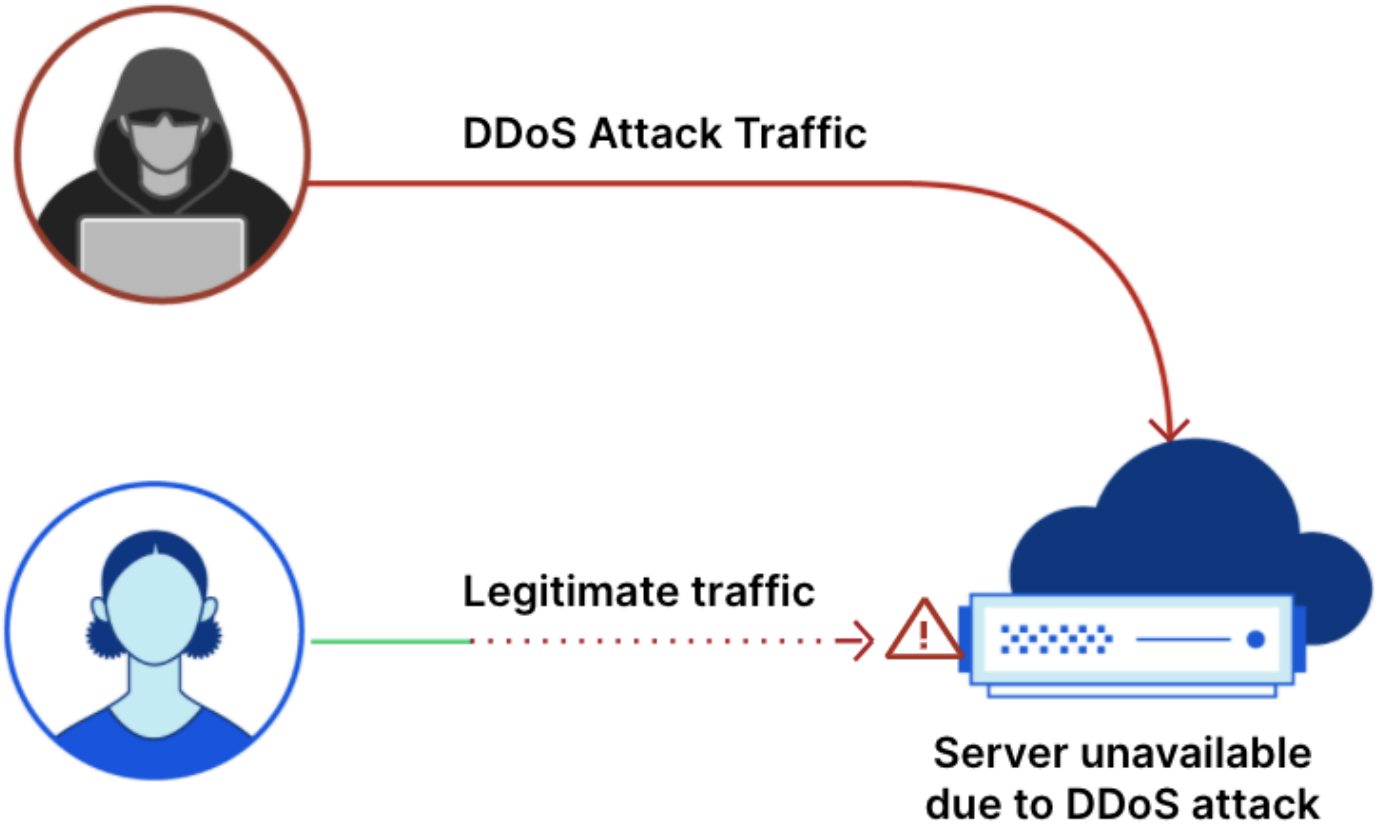
Network-layer DDoS attacks

- On the Cloudflare network, the highest DDoS activity was observed in our data centers in Rwanda, China, and Brunei.
- Almost 44% of all of the attacks in Q1 occurred in January.
- Top emerging threats include attacks targeting Jenkins and TeamSpeak3 servers, which increased by 940% and 203% QoQ, respectively.
- Additional emerging threats include floods of QUIC version negotiation packets that may have been an attempt to disrupt Cloudflare's

infrastructure.

Application-layer DDoS attacks

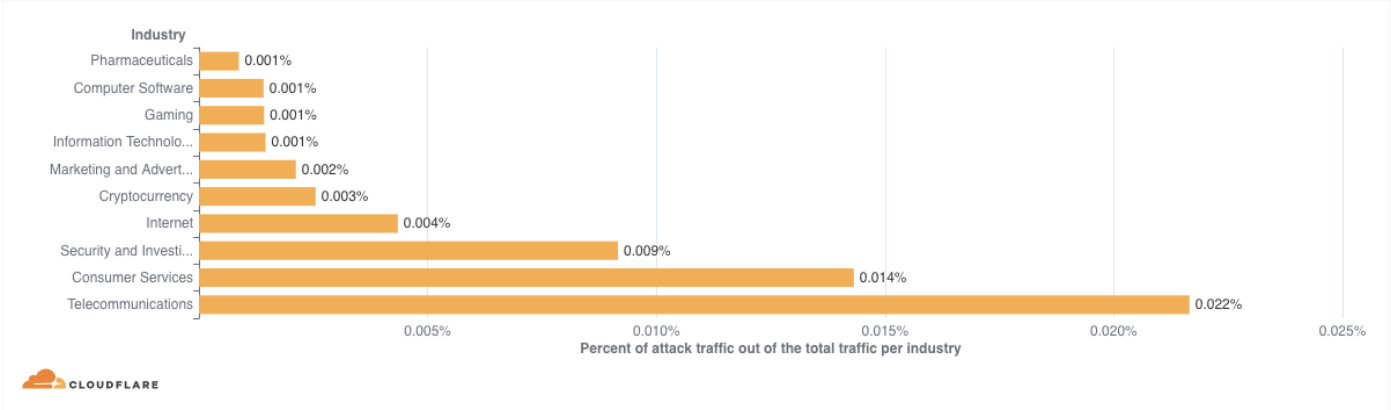
Application-layer DDoS attacks, or HTTP DDoS attacks, are attacks that aim to disrupt an HTTP server by making it unable to process requests. If a server is bombarded with more requests than it can process, the server will drop legitimate requests or even crash.



DDoS attack activity per industry

When we break down DDoS activity by our customer's market industry, we can see that Telecommunication was the most targeted industry in Q1. This is a significant jump from sixth place in 2020 Q4. Following in second place is the Consumer Services industry, and in third place the Security and Investigations industry.

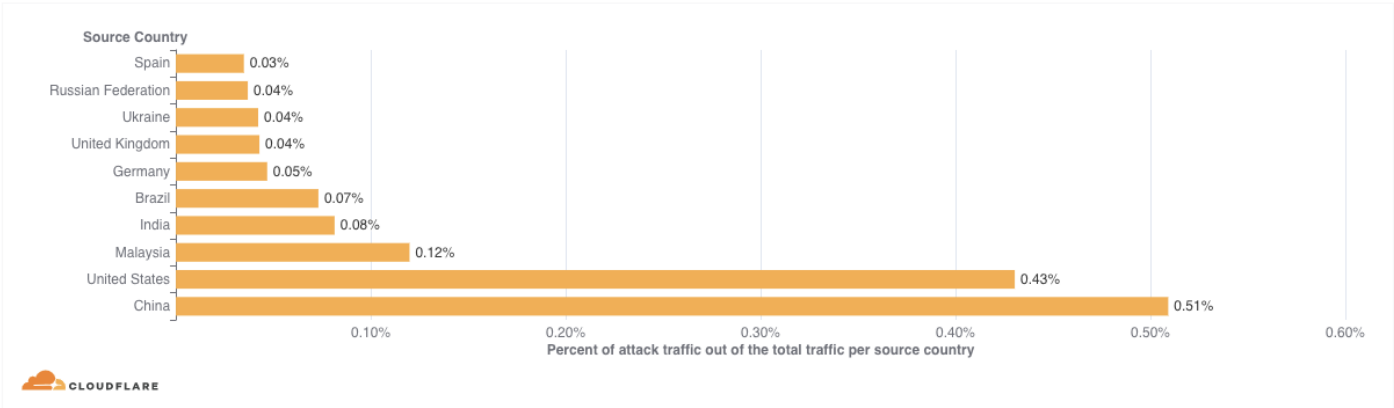
DDoS activity per industry



DDoS activity by source country

As opposed to network-layer attacks, the source IP cannot be spoofed in an HTTP attack. A connection must be established. By looking up the location of the source IP of the client, we can identify the source country. A high DDoS activity rate in a given country indicates large botnets operating from within. Both in 2020 Q4 and 2021 Q1, China came in first place, with the US not far behind.

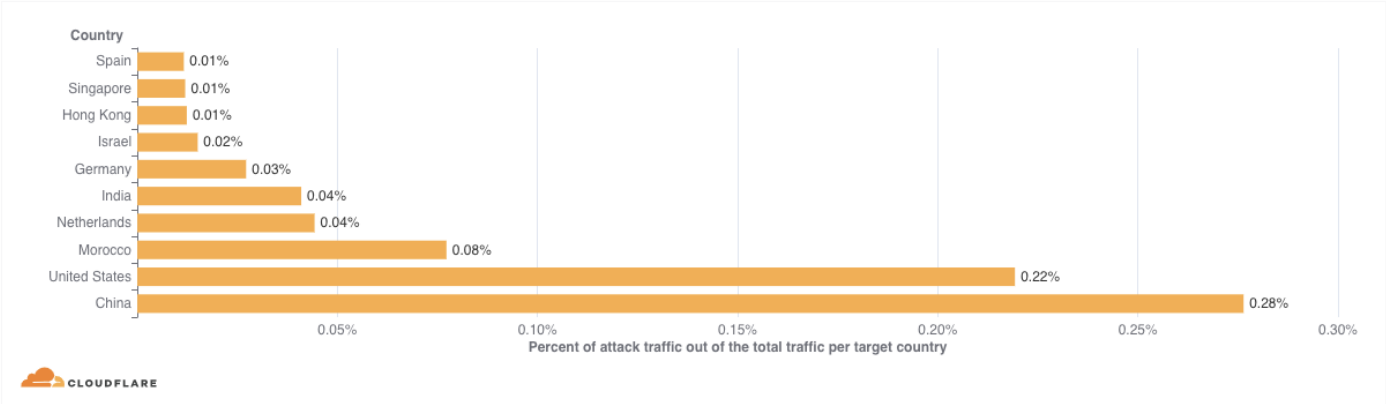
DDoS activity by source country



DDoS activity by target country

In order to identify which countries are being attacked the most, we break down the DDoS activity by our customer's billing country. Similar to the attack source breakdown, China and the US come in first and second places, respectively. Interestingly enough, in the previous quarter, India dethroned China from the first place, perhaps due to the elections in India that also occurred throughout 2020 Q4.

DDoS activity by target country

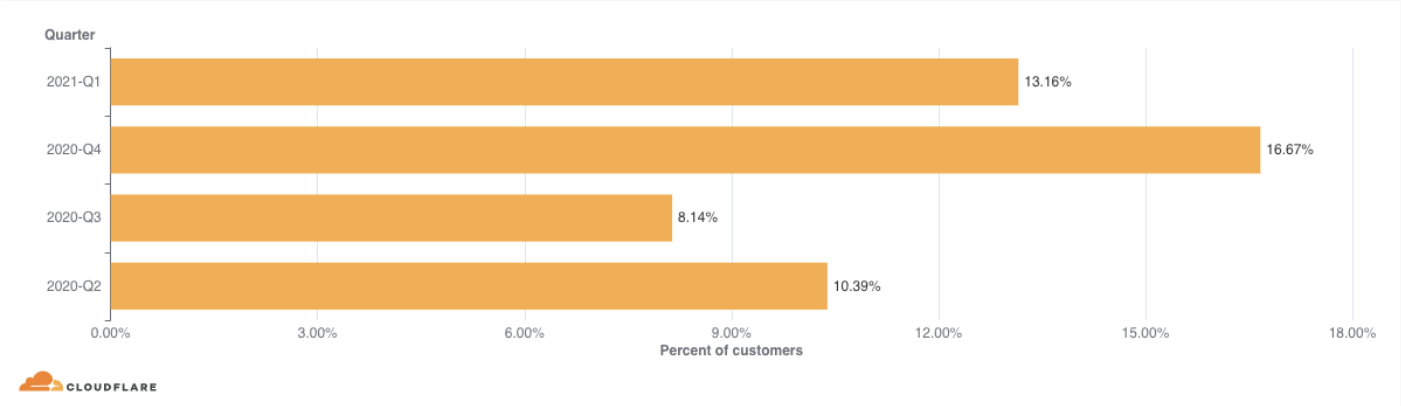


Ransom attacks

As we've seen, our customers on the non-Enterprise plans were the most targeted by DDoS attacks. However, it's not just the quantity of attacks that is high, but these customers also reported the highest number of Ransom DDoS attacks (RDDoS). In 2021 Q1, 13% of surveyed Cloudflare customers that were hit by a DDoS attack reported they were either extorted by an RDDoS attack or received a threat in advance. Of those, 62% are on the Pro plan and 33% on the Business plan. This is a continued trend from 2020 Q4 where the number of extorted customers was 17%, including a Fortune Global 500 company that was targeted by a group claiming to be the Lazarus Group, a company which we onboarded and protected.

Ransom DDOS Attacks & Threats

Percent of respondents that reported being targeted by a ransom DDoS attack

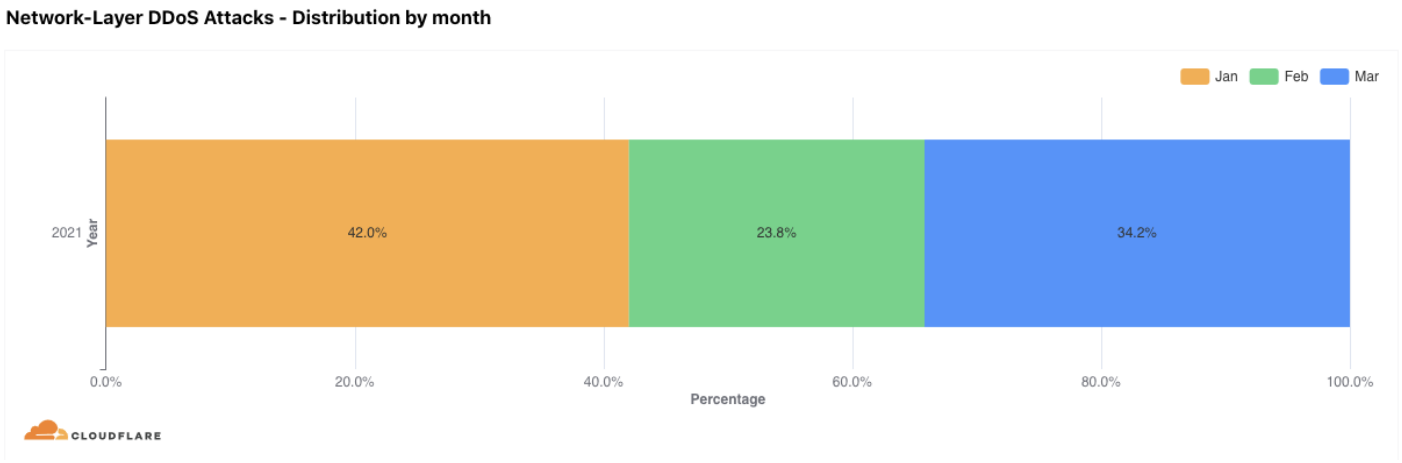


Network-layer DDoS attacks

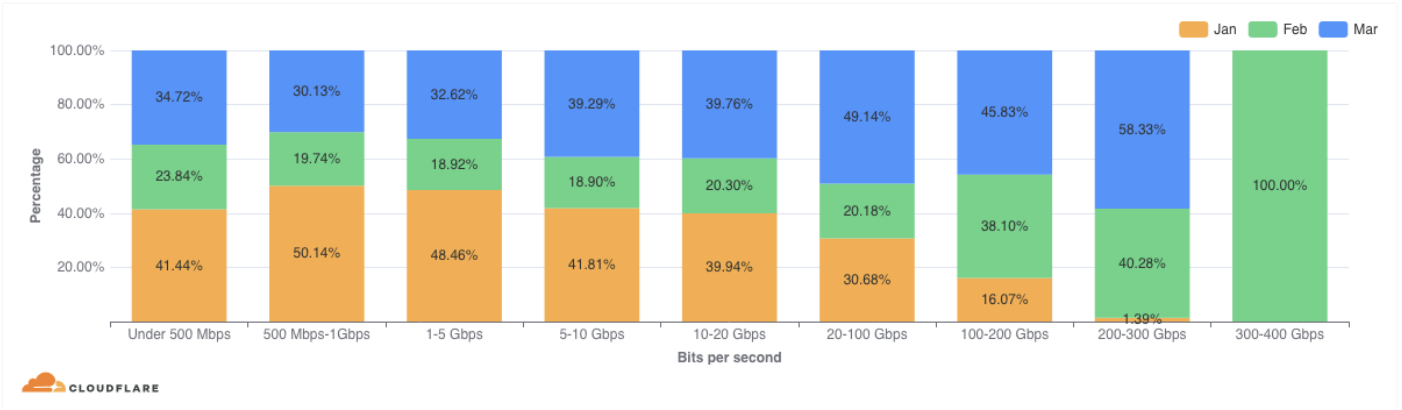
While application layer attacks strike the application (Layer 7 of the OSI model) running the service end users are trying to access, network layer attacks target exposed network infrastructure (such as in-line routers and other network servers) and the Internet link itself.

Number of attacks

On a monthly basis, January was Q1's busiest month for attackers, constituting 42% of the total attacks observed in the quarter. Followed by March with 34.2% and February with 23.8%.



In February, we did however see the largest attacks of Q1 peaking at 300-400 Gbps.



Size of attacks

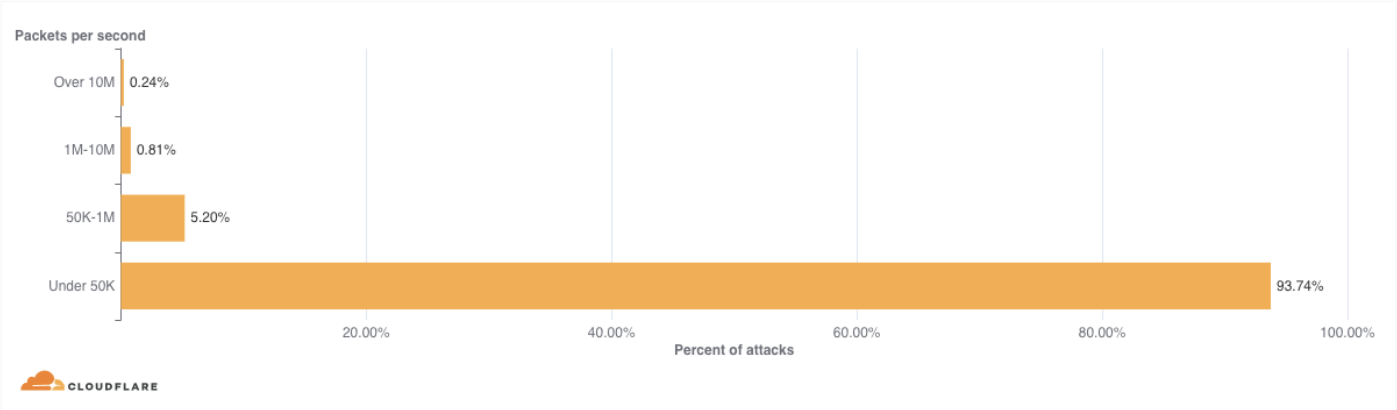
There are different ways of measuring a L3/4 DDoS attack's size. One is the volume of traffic it delivers, measured as the bit rate (specifically, gigabits-per-second). Another is the number of packets it delivers, measured as the packet rate (specifically, packets-per-second). Attacks with high bit rates attempt to saturate the Internet link, while attacks with high packet rates attempt to overwhelm the routers or other in-line hardware devices.

In 2021 Q1, a vast majority (over 97%) of the L3/4 attacks observed were smaller than 1 mpps and 500 Mbps.

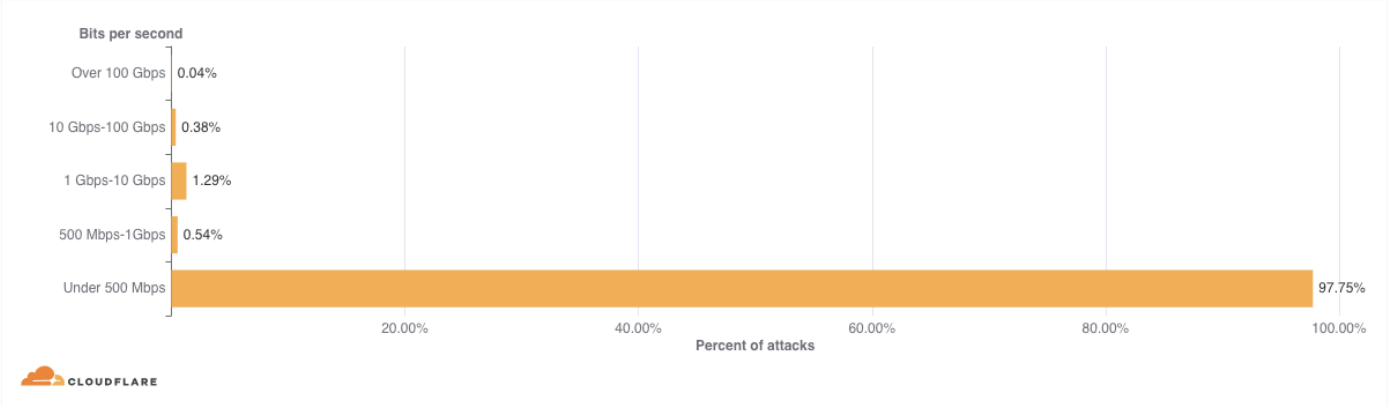
This is a continuation of the trend we observed all of last year. However, this does not imply that these attacks are harmless.

Attacks under 500 Mbps are often sufficient to create major disruptions for Internet properties that are not protected by a cloud-based DDoS protection service. Many organizations have uplinks provided by their service providers with less bandwidth capacity than 1 Gbps. Assuming their public facing network interface also serves legitimate traffic, you can see how even DDoS attacks under 500 Mbps can easily take down Internet properties.

Network-layer DDoS attacks: Distribution by packet rate



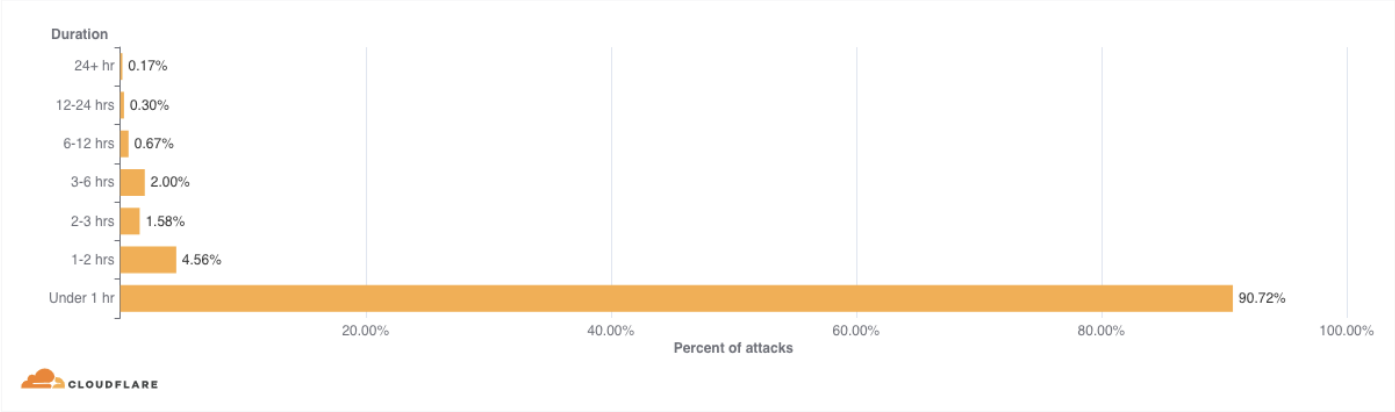
Network-layer DDoS attacks: Distribution by bit rate



Duration of attacks

Over 90% of attacks lasted under one hour in duration. Short burst attacks may attempt to cause damage without being detected by DDoS detection systems. DDoS services that rely on manual analysis and mitigation may prove to be useless against these types of attacks because they are over before the analyst can even identify the attack traffic.

Network-layer DDoS attacks: Distribution by duration



Short attacks are often also used to probe the cyber defenses of the target. Load-testing tools and automated DDoS tools, widely available on the dark web, can generate short bursts of, say, a SYN flood, and then following up with another short attack using an alternate attack vector. This allows attackers to understand the security posture of their targets before they decide to potentially launch larger attacks at larger rates and longer durations.

Attack vectors

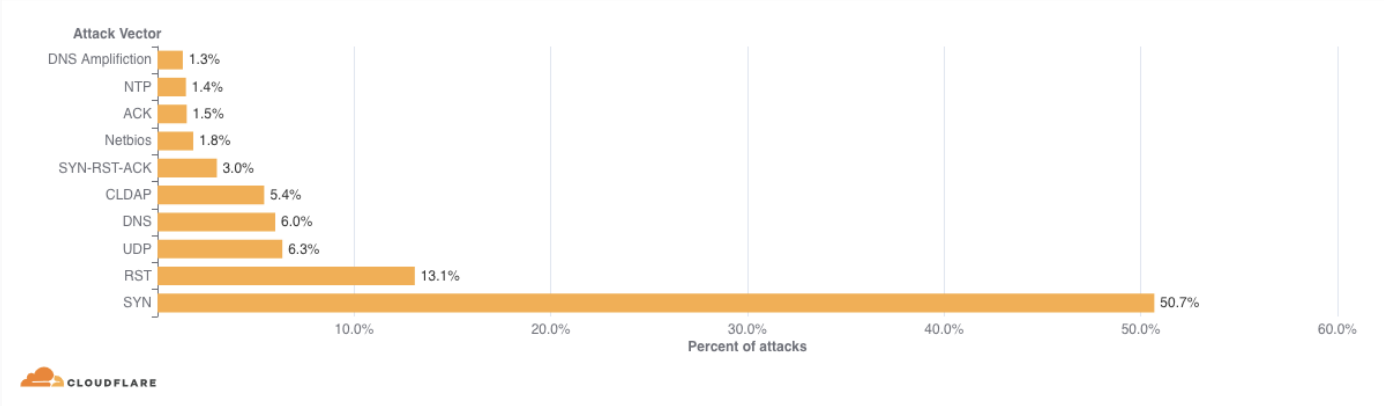
An attack vector is the attack method that the attacker utilizes. In 2021 Q1, SYN attacks continued to remain the most popular attack vector used by attackers, followed by RST, UDP, and DNS amplification attacks.

What is a SYN flood attack? It's a DDoS attack that exploits the very foundation of a TCP connection. A stateful TCP connection between a client and a server begins with a 3-way TCP handshake. The client sends an initial connection request packet with a synchronize flag (SYN). The server responds with a packet that contains a synchronized acknowledgment flag (SYN-ACK). Finally, the client responds with an acknowledgment (ACK) packet. At this point, a connection is established and data can be exchanged until the connection is closed. This stateful process can be abused by attackers to cause denial of service events.

By repeatedly sending SYN packets, the attacker attempts to overwhelm a server or the router's connection table that tracks the state of TCP connections. The router replies with a SYN-ACK packet, allocates a certain amount of memory for each given connection, and falsely waits for the client to respond with the final ACK. Given a sufficient number of connections occupying the router's memory, the router is unable to allocate more memory for legitimate clients, causing the router to crash or preventing it from handling legitimate client connections, i.e., a denial of service event.

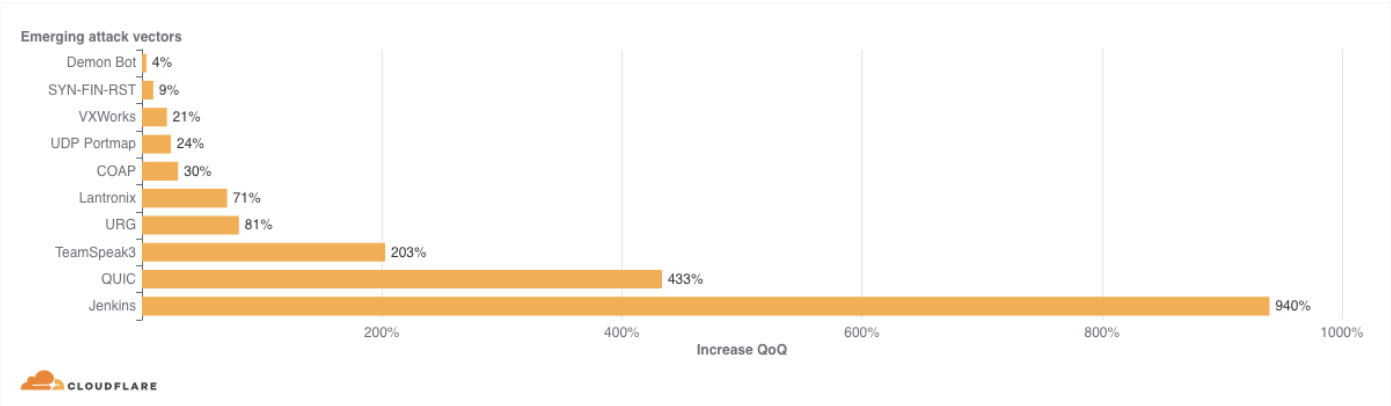
Similarly, a RST amplification flood attack exhausts the target servers by depleting their system resources used to look up incoming packets for a current session.

Network-layer DDoS attacks: Distribution by top attack vectors



Emerging threats

Network-layer DDoS attacks: Top emerging threat vectors



While SYN attacks remain popular, this quarter we've seen an enormous uptick of 940% in attacks targeting Jenkins servers. Jenkins is a free open-source automation server. It helps engineering teams facilitate software development. A vulnerability in an older version of the server (Jenkins 2.218 and earlier) aided the launch of DDoS attacks. This vulnerability was fixed in Jenkins 2.219 by disabling UDP multicast/broadcast messages by default. However, there are still many vulnerable and exposed devices running UDP-based services which are being harnessed to generate volumetric amplification attacks.

Cloudflare also observed a 433% increase in L3/4 DDoS attacks over the QUIC protocol, a new encrypted-by-default Internet transport protocol that runs over UDP. Version negotiations packets sent by a server to client allow the server to indicate the version of QUIC it supports to the client. Since UDP is stateless, it is

easy for attackers to mimic Version Negotiation packets by spoofing the source IP address and overwhelm a client.

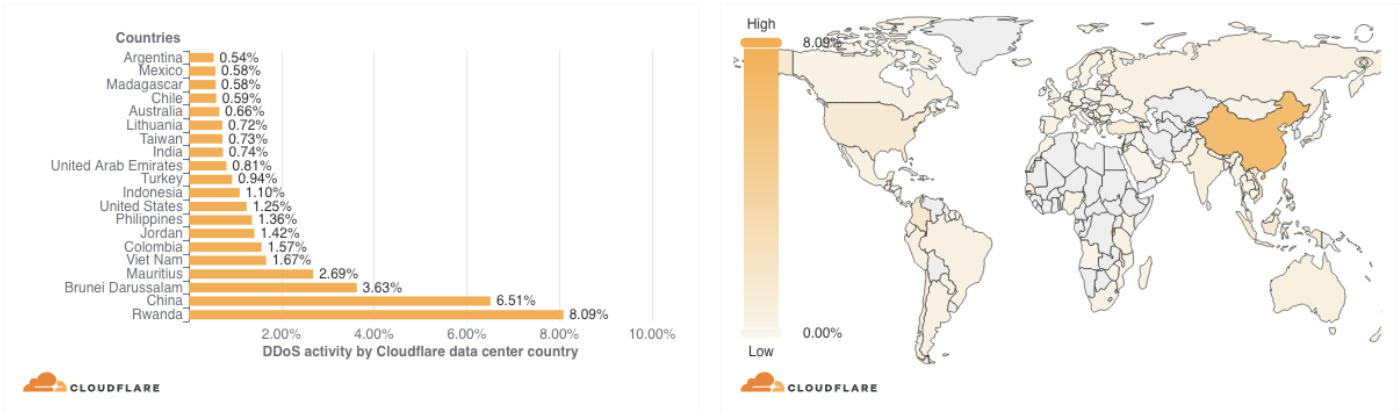
The attacks targeting Cloudflare may have meant to impact Cloudflare's infrastructure — perhaps by downgrading the versions being used — rather than targeting specific customers. You can learn more about QUIC amplification attacks here.

The third emerging threat vector observed was TeamSpeak, a proprietary voice-over-Internet Protocol (VoIP) that runs over UDP to help gamers talk with other gamers in real time. This emerging threat increased by 203% QoQ.Talking instead of just chatting can significantly improve a gaming team's efficiency and help them win. DDoS attacks that target TeamSpeak servers may be launched by rival groups in an attempt to disrupt their communication path during real-time multiplayer games and thus impact their team's performance.

DDoS activity by Cloudflare data center country

Looking at country-based distribution for network layer DDoS attacks, Rwanda, China, and Brunei observed the most number of L3/4 DDoS attacks. Unlike application layer DDoS attacks, attackers can (and typically do) spoof the source IP address to obfuscate the source location of the DDoS attack. For this reason, when analyzing L3/4 DDoS attacks, we bucket the traffic by the Cloudflare edge data center locations where the traffic was ingested, and not by the location of the source IP. Cloudflare is able to overcome the challenges of spoofed IPs by displaying the attack data by the location of Cloudflare's data center in which the attack was observed. We're able to achieve geographical accuracy in our report because we have data centers in over 200 cities around the world.

DDoS Activity by Cloudflare data center country



To view all regions and countries, check out the Radar DDoS Report dashboard's interactive map.

Helping build a better Internet

Cloudflare was founded with the mission to help build a better Internet — one where the impact of DDoS attacks is a thing of the past. Over the last 10 years, we have been unwavering in our efforts to protect our customers' Internet properties from DDoS attacks of any size or kind. CCP Games and Panasonic are two of many customers that benefit from Cloudflare's DDoS Protection.

Cloudflare was also recently named a leader in The Forrester WaveTM: DDoS Mitigation Solutions, Q1 2021. You can download a complimentary copy of the report here.

According to the report, written by Forrester Senior Analyst for Security and Risk, David Holmes, "Cloudflare protects against DDoS from the edge, and fast... customer references view Cloudflare's edge network as a compelling way to protect and deliver applications."

There are three key reasons Cloudflare DDoS Protection is recognized by customer and industry analysts alike:

1. **Cloudflare's network architecture**: Cloudflare doesn't operate scrubbing centers, as we believe that the scrubbing center model is a

flawed approach to DDoS protection. Scrubbing centers cause delays and cost too much to build and run. Instead, we run DDoS protection from every server in every data center in our network. Our Anycast-based architecture makes our capacity equivalent to our DDoS scrubbing capacity, the largest in the market at 59 Tbps. This means Cloudflare detects and mitigates DDoS attacks close to the source of attack. Better yet, Cloudflare's global threat intelligence acts like an immune system for the Internet — employing our machine learning models to learn from and mitigate attacks against any customer to protect them all.

2. **Fast performance**: Our customers constantly tell us that they want robust security but not at the expense of performance. From its inception, Cloudflare was architected so that customers do not incur a latency penalty as a result of attacks. Our Anycast architecture allows us to mitigate attacks closest to the source and analyze traffic out-of-path, ensuring that our DDoS mitigation solution doesn't add any latency to legitimate traffic. The rule is applied at the most optimal place in the Linux stack for a cost efficient mitigation, ensuring that there's no performance penalty. Performance tests over Cloudflare's network show that the latency decreased by 3 ms and packet loss was nearly zero when traffic was routed over Cloudflare Magic Transit.
3. **Cloudflare's support**: Every Cloudflare enterprise customer account is assigned a team (including an Account Executive, Solution Engineer, and Customer Success Manager) that actively supports customers through onboarding and beyond to help identify areas for optimization in customer configurations.

Cloudflare's 24x7x365 global "follow the sun" support team is always ready to pick up the phone and provide instant human response when our enterprise customers request urgent support.

To quote Grant Ingersoll, CTO of the Wikimedia Foundation, “Cloudflare has reliable infrastructure and an extremely competent and responsive team. They are well-positioned to deflect even the largest of attacks.”

To learn more about Cloudflare’s DDoS solution contact us or get started.

We protect entire corporate networks, help customers build Internet-scale applications efficiently, accelerate any website or Internet application, ward off DDoS attacks, keep hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

DDoS Trends Security DDoS Reports