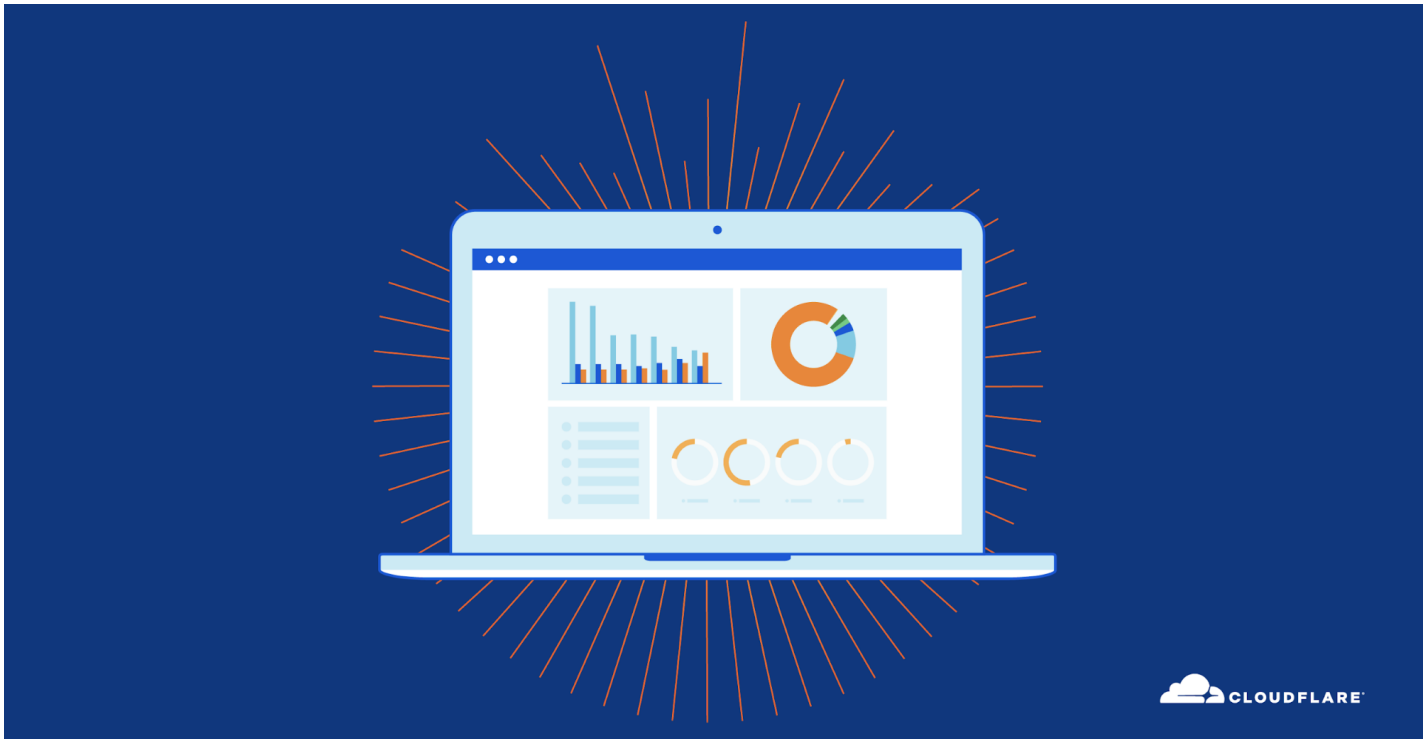
DDoS attack trends for 2021 Q2

07/20/2021

 Vivek Ganti  Omer Yoachimik

14 min read

This post is also available in 简体中文, 繁體中文, 日本語, 한국어, Deutsch and Français.



Recent weeks have witnessed massive ransomware and ransom DDoS (Distributed Denial of Service) attack campaigns that interrupted aspects of critical infrastructure around the world, including one of the largest petroleum pipeline system operators, and one of the world's biggest meat processing companies. Earlier this quarter, more than 200 organizations across Belgium, including the government and parliament websites and other services, were also DDoS'd.

And when most of the United States were celebrating Independence Day on July 4, hundreds of US companies were hit by a ransomware attack demanding 70

million USD in Bitcoin. Attackers known to be affiliated with REvil, a Russian ransomware group, exploited multiple previously unknown vulnerabilities in IT management software. The targets included schools, small public-sector bodies, travel and leisure organizations, and credit unions, to name a few. While the threat of ransomware and ransom DDoS is not new (read our posts on ransomware and ransom DDoS from 2021 Q1), the latest attacks on Internet properties ranging from wineries, professional sports teams, ferry services and hospitals has brought them from just being background noise to front page headlines affecting our day-to-day lives. In fact, recent attacks have propelled ransomware and DDoS to the top of US President Biden's national security agenda.

The DDoS attack trends observed over Cloudflare's network in 2021 Q2 paint a picture that reflects the overall global cyber threat landscape. Here are some highlights.

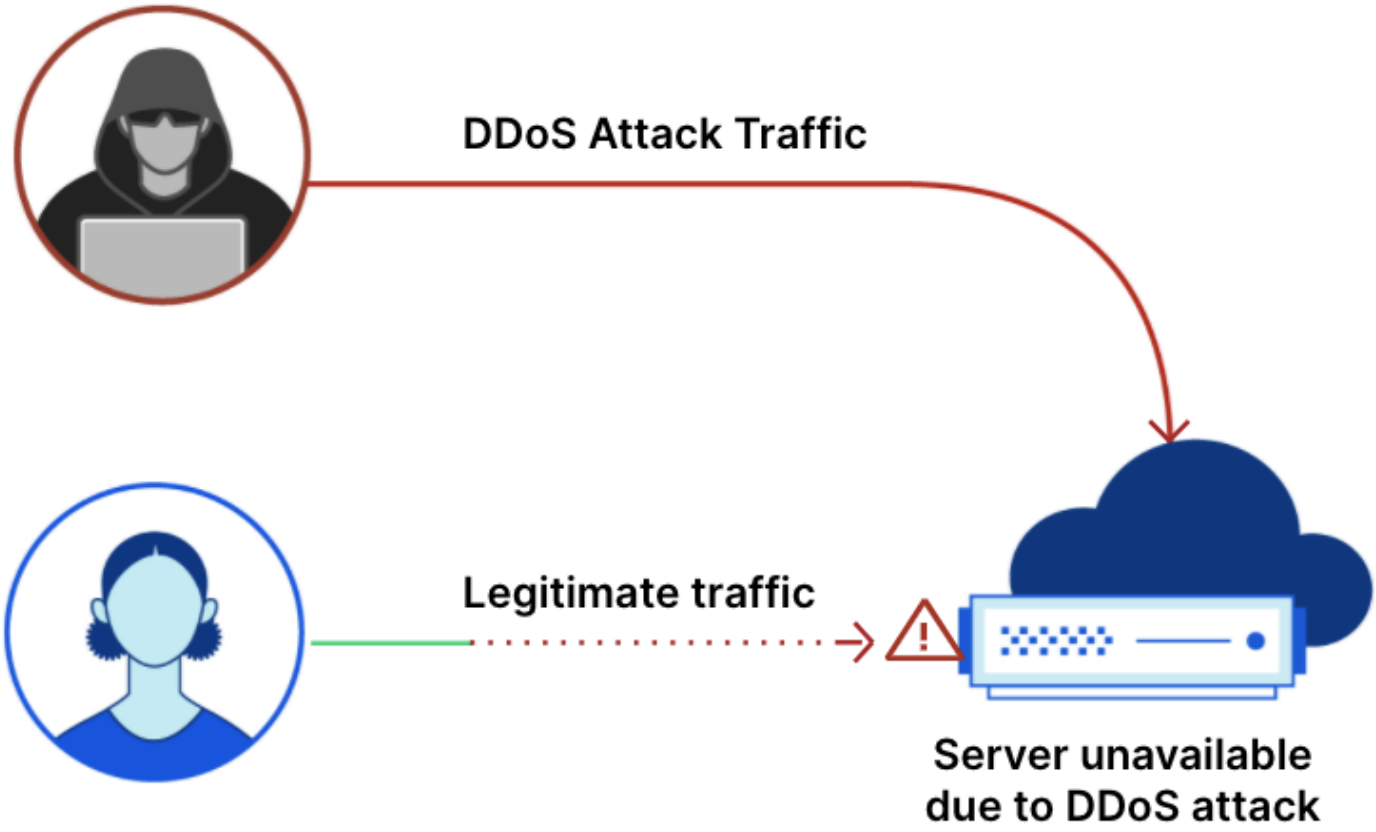
- Over 11% of our surveyed customers who were targeted by a DDoS attack reported receiving a threat or ransom letter threatening in advance, in the first six months of this year. Emergency onboarding of customers under an active DDoS attack increased by 41.8% in 2021 H1 compared to 2020 H2.
- HTTP DDoS attacks targeting government administration/public sector websites increased by 491%, making it the second most targeted industry after Consumer Services whose DDoS activity increased by 684% QoQ.
- China remains the country with the most DDoS activity originating from within their borders — 7 out of every 1,000 HTTP requests originating from China were part of an HTTP DDoS attack targeting websites, and more than 3 out of every 100 bytes that were ingested in our data centers in China were part of a network-layer DDoS attack.

- Emerging threats included amplification DDoS attacks that abused the Quote of the Day (QOTD) protocol which increased by 123% QoQ. Additionally, as the adoption of QUIC protocol continues to increase, so do attacks over QUIC — registering a whopping 109% QoQ surge in 2021 Q2. The number of network-layer DDoS attacks in the range of 10-100 Gbps increased by 21.4% QoQ. One customer that was attacked is Hypixel, an American gaming company. Hypixel remained online with no downtime and no performance penalties to their gamer users, even when under an active DDoS attack campaign larger than 620 Gbps. Read their story here.

To view all DDoS attack insights across all regions and industries worldwide, visit Cloudflare's interactive Radar DDoS dashboard.

Application-layer DDoS attacks

Application-layer DDoS attacks, specifically HTTP DDoS attacks, are attacks that usually aim to disrupt an HTTP server by making it unable to process legitimate user requests. If a server is bombarded with more requests than it can process, the server will drop legitimate requests or even crash resulting in performance penalties or a denial of service event for legitimate users.

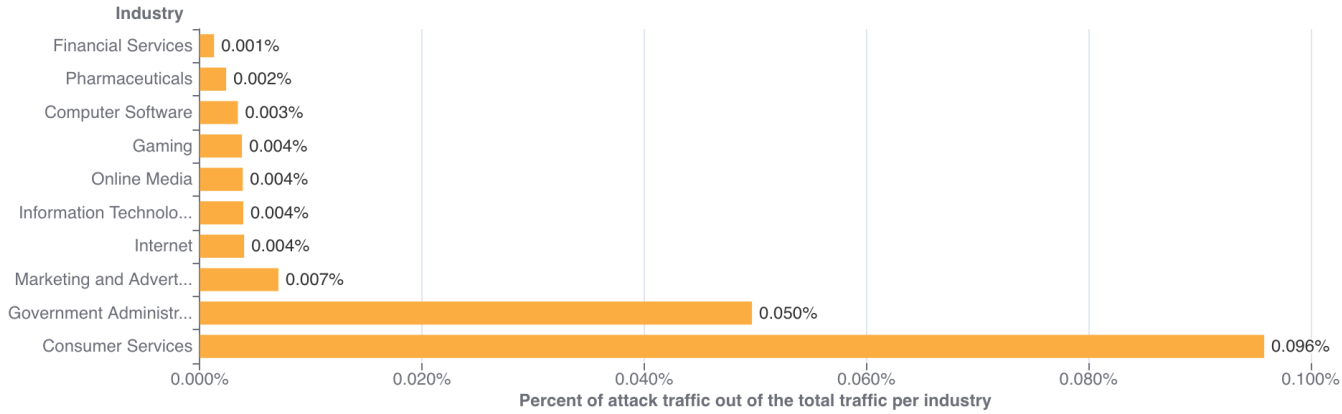


DDoS activity per market industry

When we analyze attacks, we calculate the ‘DDoS activity’ rate, which is the percentage 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 larger data center that naturally handles more traffic and therefore also more attacks.

In 2021 Q2, Consumer Services was the most targeted industry followed by Government Administration and Marketing & Advertising.

DDoS activity per industry



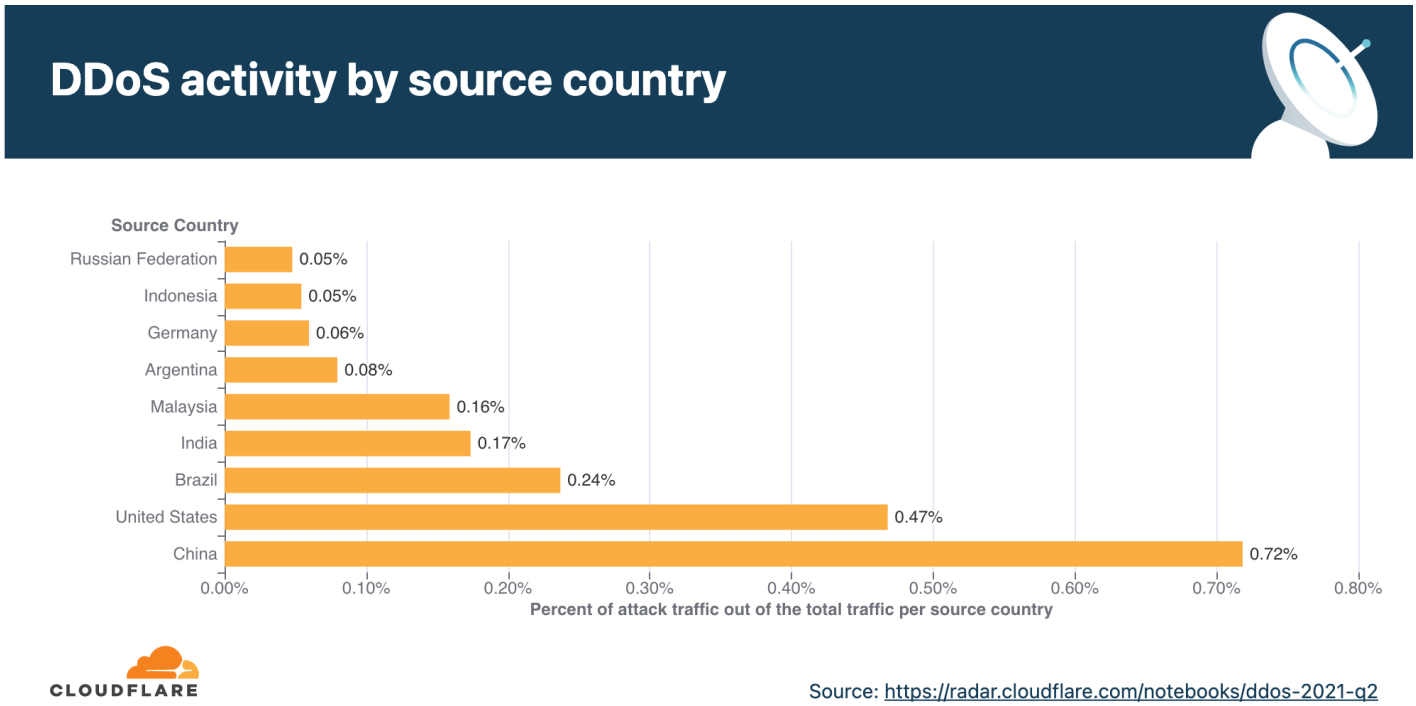
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

DDoS activity per source country

To understand the origin of the HTTP attacks we observed over Cloudflare's network, we look at the source IP address of the client generating the attack HTTP requests. Unlike network-layer attacks, source IPs cannot be spoofed in HTTP attacks. A high DDoS activity rate in a given country indicates large botnets operating from within.

China and the US remain in the first and second places, respectively, regarding the percentage of DDoS activity originating from within their territories. In China, more than 7 out of every 1,000 HTTP requests were part of an HTTP DDoS attack, while in the US almost 5 out of 1,000 HTTP requests were part of an attack.

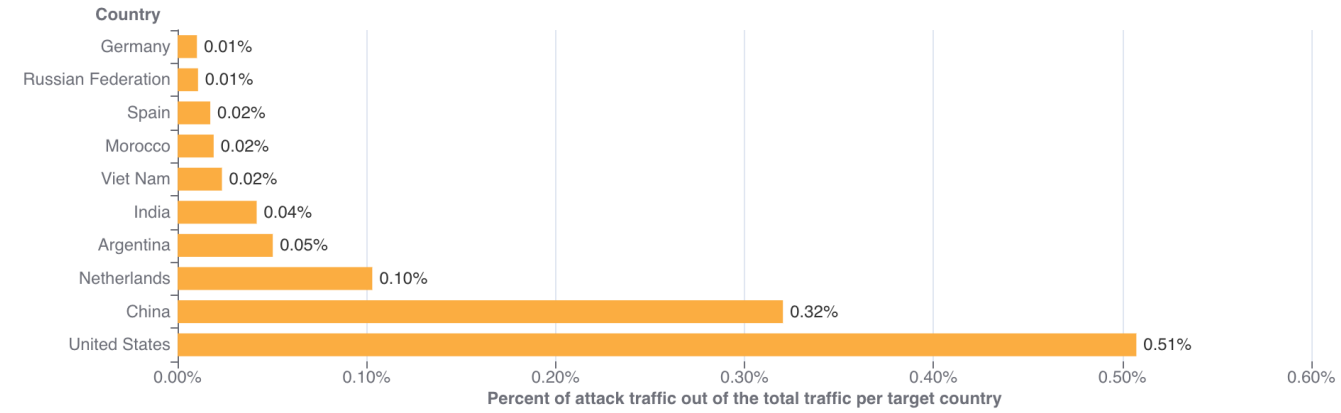


DDoS activity per target country

In order to identify which countries the targets of the DDoS attacks resided in, we break down the DDoS activity by our customers' billing countries. Note that Cloudflare does not charge for attack traffic and has pioneered providing unmetered and unlimited DDoS protection since 2017. By cross-referencing the attack data with our customers' billing country, we can identify which countries were attacked the most.

Data observed in 2021 Q2 suggest that organizations in the US and China were the most targeted by HTTP DDoS attacks. In fact, one out of every 200 HTTP requests destined to US-based organizations was part of a DDoS attack.

DDoS activity by target country



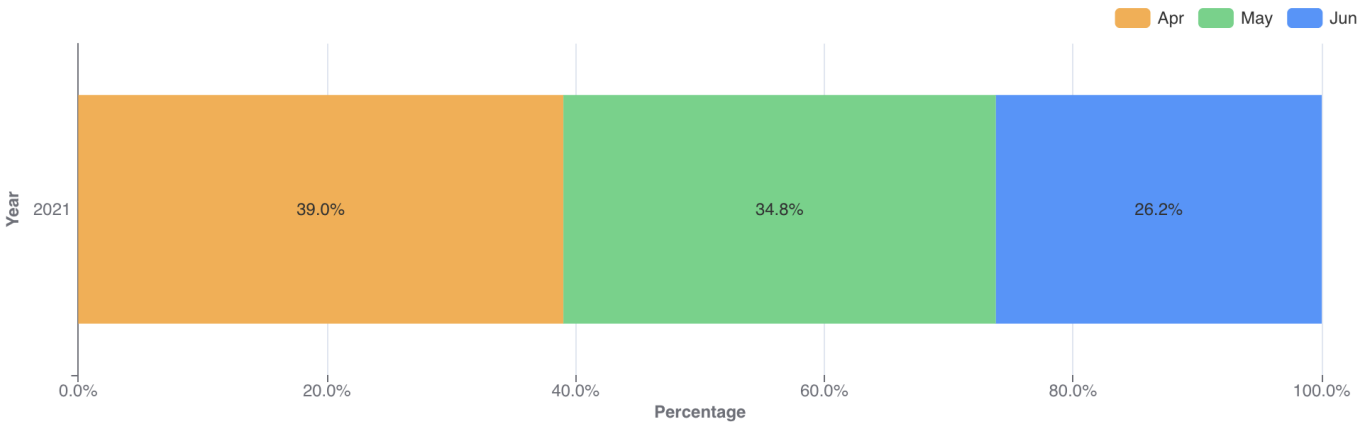
CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

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 network infrastructure (such as in-line routers and other network servers) and the Internet link itself.

Network-Layer DDoS Attacks - Distribution by month



CLOUDFLARE

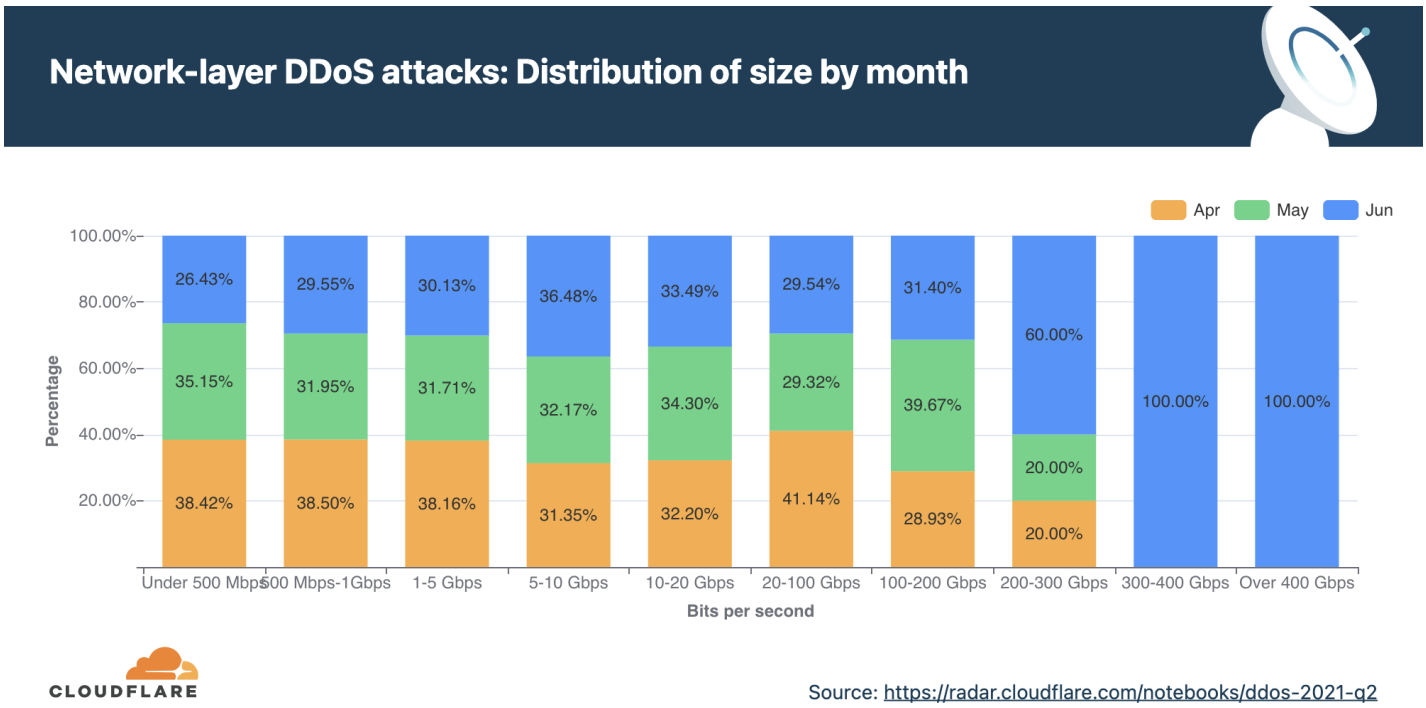
Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

The chart above shows the distribution of network-layer DDoS attacks in 2021 Q2.

Distribution of attacks by size (packet rate and bit rate)

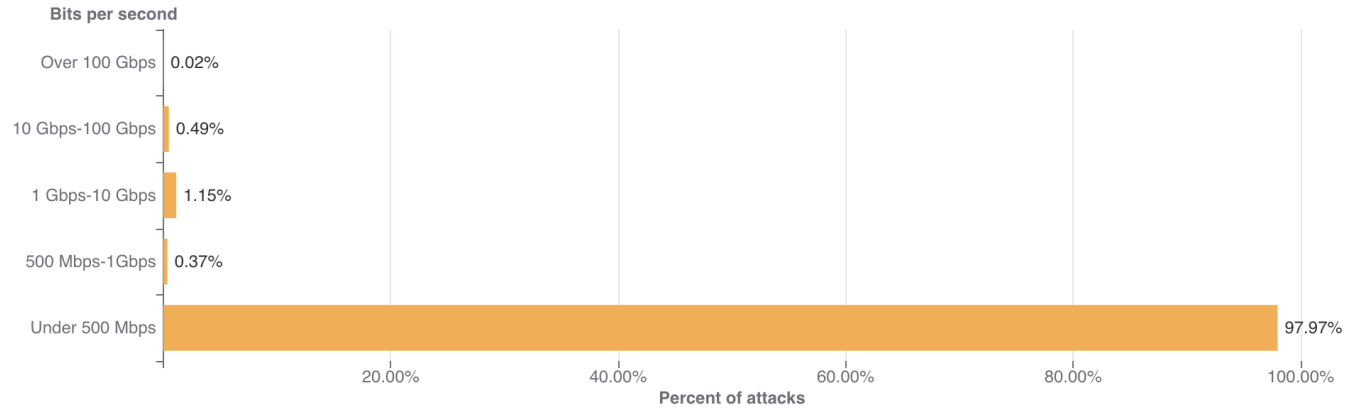
There are different ways of measuring the size of a L3/4 DDoS attack. One is the volume of traffic it delivers, measured as the bit rate (specifically, gigabits-per-second). Another is the number of packets it delivers, measured as the packet rate (specifically, packets-per-second). Attacks with high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

The distribution of attacks by their size (in bit rate) and month is shown below. As observed in the chart, all attacks over 300 Gbps were observed in the month of June.



In terms of bit rate, attacks under 500 Mbps constituted a majority of all DDoS attacks observed in 2021 Q2.

Network-layer DDoS attacks: Distribution by bit rate

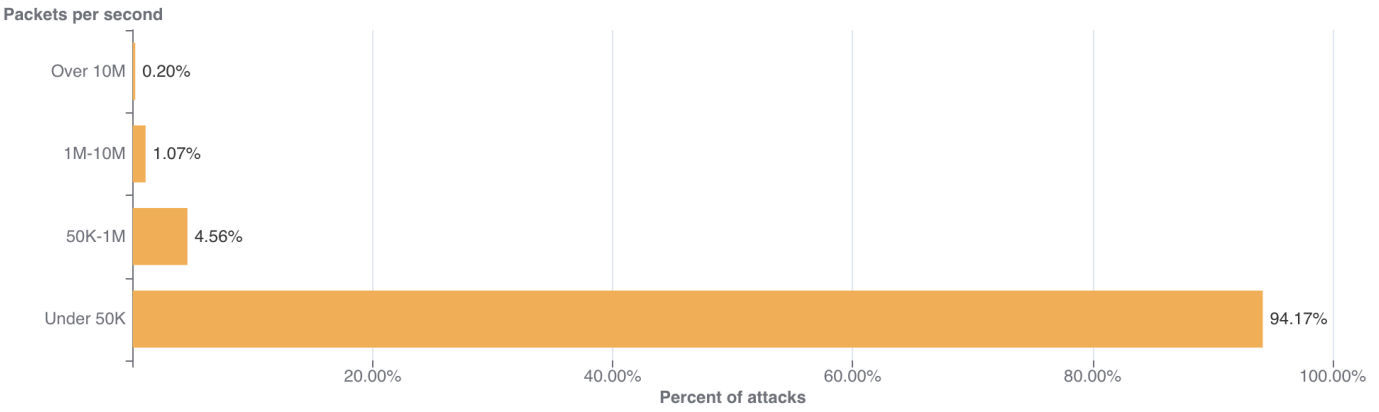


CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

Similarly, looking from the lens of packet rate, nearly 94% of attacks were under 50K pps. Even though attacks from 1-10M pps constituted only 1% of all DDoS attacks observed, this number is 27.5% higher than that observed in the previous quarter, suggesting that larger attacks are not diminishing either -- but rather increasing.

Network-layer DDoS attacks: Distribution by packet rate



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

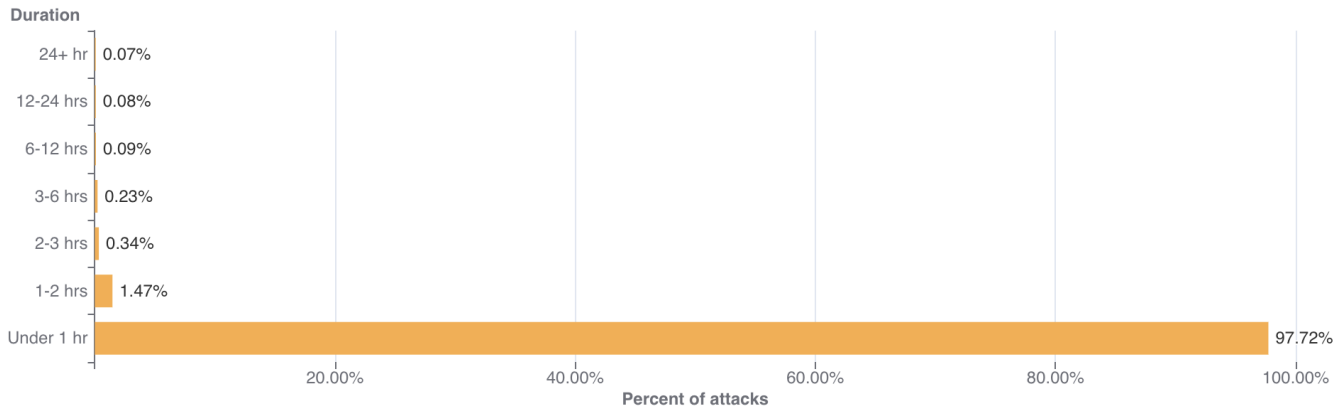
Note that while attacks under 500 Mbps and 50K pps might seem ‘small’ compared to other headline-making large attacks, they are often sufficient to create major disruptions for Internet properties that are not protected by an always-on, automated cloud-based DDoS protection service. Moreso, many organisations have uplinks provided by their service providers with a bandwidth capacity smaller than 1 Gbps. Assuming their public-facing network interface also serves legitimate traffic, DDoS attacks smaller than 500 Mbps are often capable of taking down exposed Internet properties.

Distribution by attack duration

Cloudflare continues to see a large percentage of DDoS attacks that last under an hour. In Q2, over 97% of all DDoS attacks lasted less than an hour.

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 even identifies the attack traffic.

Network-layer DDoS attacks: Distribution by duration



CLOUDFLARE

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

Alternatively, the use of short attacks may be used to probe the cyber defenses of the target. Load-testing tools and automated DDoS tools, that are widely available on the dark web, can generate short bursts of a SYN flood, for example, and then follow up with another short attack using a different attack vector. This allows attackers to understand the security posture of their targets before they decide to launch larger attacks at larger rates and longer durations — which come at a cost.

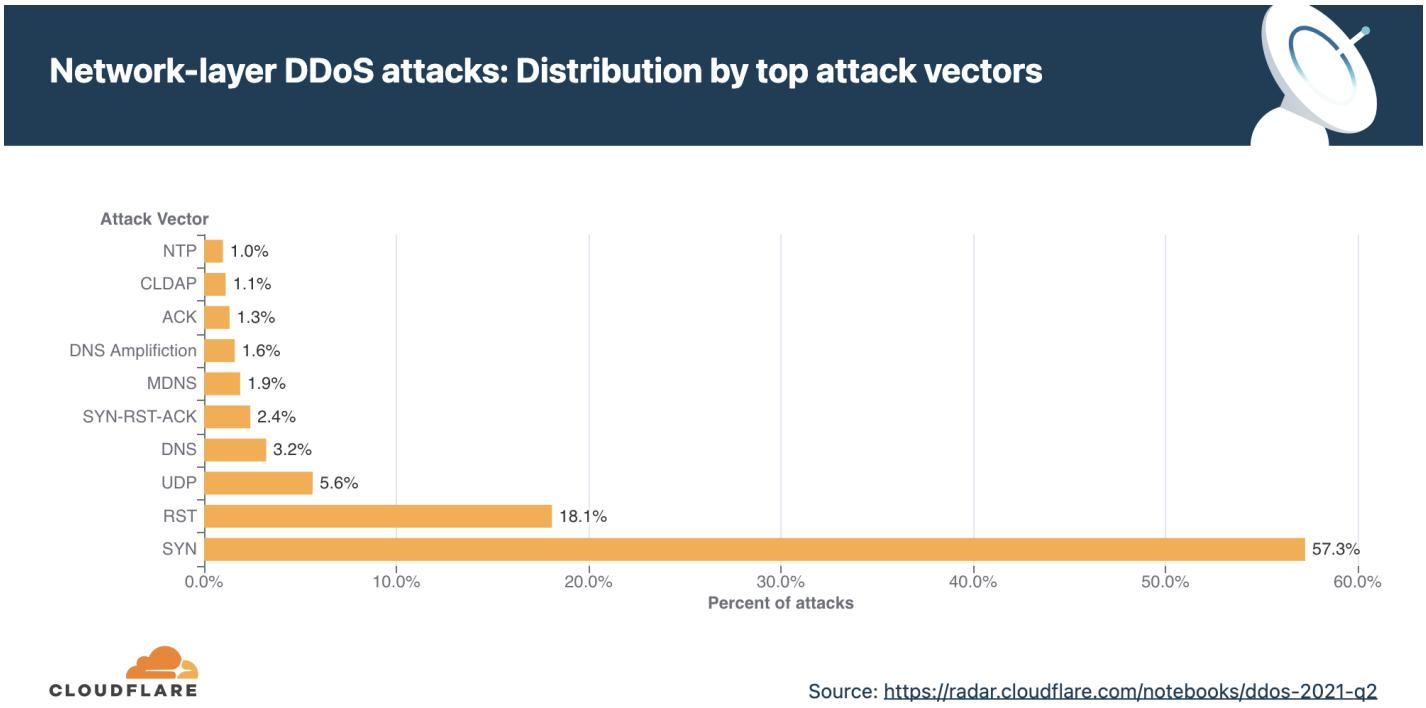
In other cases, attackers generate small DDoS attacks as proof and warning to the target organization of the attacker's ability to cause real damage later on. It's often followed by a ransom email to the target organization, demanding payment to avoid suffering an attack that could more thoroughly cripple network infrastructure.

This highlights the need for an always on, automated DDoS protection approach. DDoS protection services that rely on manual re-routing, 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.

Distribution of attacks by attack vectors

An attack vector is the term used to describe the method that the attacker utilizes in their attempt to cause a denial of service event.

As observed in previous quarters, attacks utilizing SYN floods and UDP-based protocols remain the most popular methods by attackers.



What is a SYN flood attack? It's a DDoS attack that exploits the very foundation of the TCP protocol. 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 further memory for legitimate clients, causing the router to crash or preventing it from handling legitimate client connections, i.e., a denial of service event.

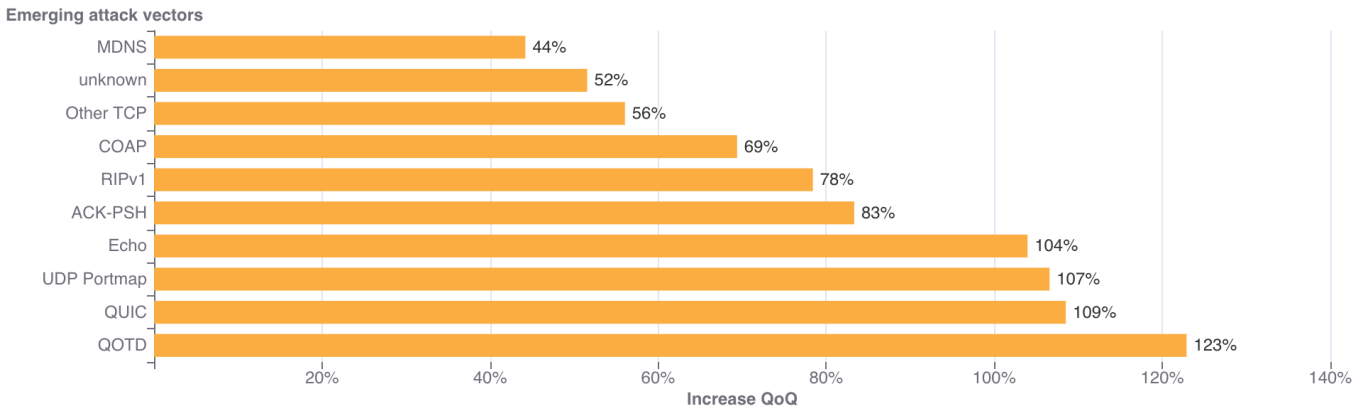
Emerging threats

Emerging threats included amplification DDoS attacks that abuse the Quote of the Day (QOTD) service which increased by 123% QoQ. QOTD was defined in RFC-865 (1983) and can be sent over either the UDP or TCP protocols. It was originally designed for debugging and as a measurement tool, with no specific syntax for the quote. The RFC does however recommend the use of ASCII characters and to limit the length to 512 characters.

Furthermore, we've seen a 107% increase QoQ in UDP Portmap and Echo attacks -- all of which are really old attack vectors. This may indicate attackers digging up old methods and attack tools to try and overcome protection systems.

As we've seen in previous quarters, the adoption of the QUIC protocol continues to increase. Consequently, so do attacks over QUIC, or more specifically floods and amplification attacks of non-QUIC traffic in places where we'd expect to see QUIC traffic. In 2021 Q2, these types of attacks increased by 109% QoQ. This continued trend may indicate that attackers are attempting to abuse the QUIC-designated ports and gateways into organizations' networks -- searching for vulnerabilities and security holes.

Network-layer DDoS attacks: Top emerging threat vectors



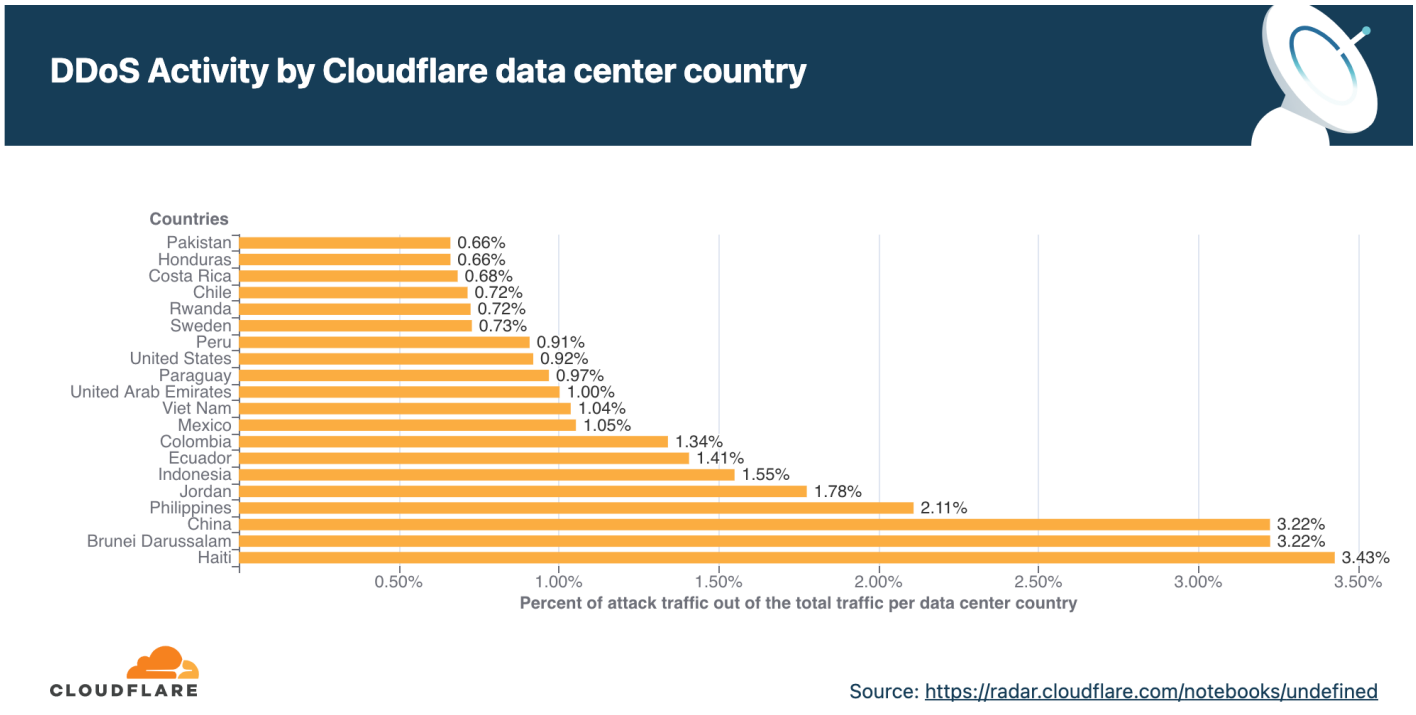
CLOUDFLARE

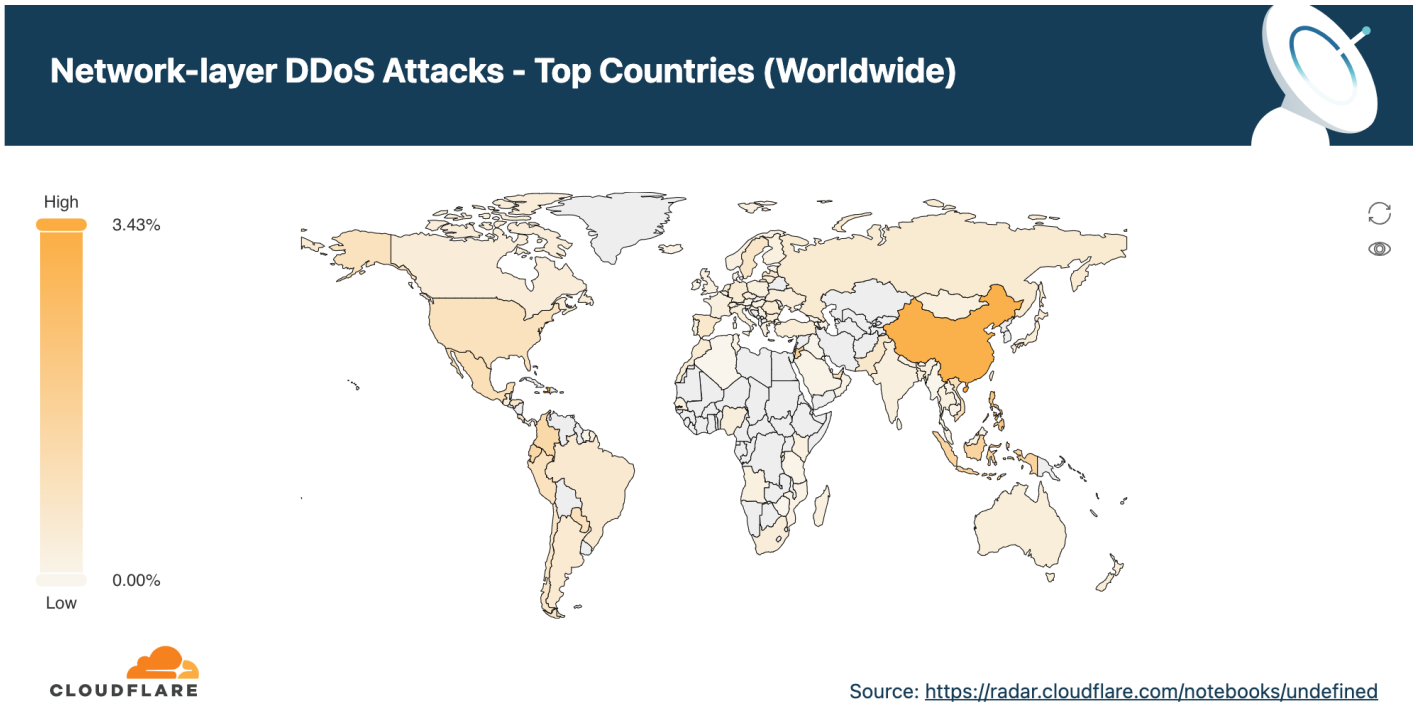
Source: https://radar.cloudflare.com/notebooks/ddos-2021-q2

DDoS activity by Cloudflare data center country

In 2021 Q2, our data center in Haiti observed the largest percentage of network-layer DDoS attack traffic, followed by Brunei (almost 3 out of every 100 packets were part of an attack) and China.

Note that when analyzing network-layer DDoS attacks, we bucket the traffic by the Cloudflare edge data center locations where the traffic was ingested, and not by the source IP. The reason for this is that, when attackers launch network-layer attacks, they can spoof the source IP address in order to obfuscate the attack source and introduce randomness into the attack properties, which may make it harder for simple DDoS protection systems to block the attack. Hence, if we were to derive the source country based on a spoofed source IP, we would get a spoofed country. 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.





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

A note on ransomware and ransom DDoS — a growing global threat

The last few weeks have seen a resurgence of ransom-driven cyber threats: ransomware and ransom DDoS (RDDoS).

So what is ransomware and ransom DDoS, and how are they different?

Ransomware is malicious software that encrypts an organization's systems and databases, rendering them inaccessible and unusable. Malware is usually introduced into an organization's systems via phishing emails -- tricking employees to click on a link or download a file. Once the malware is installed on the employee's device, it encrypts the device and can propagate to the entire network of the organization's servers and employee devices. The attacker will

demand money, usually in the form of Bitcoin, in exchange for decrypting the organization's systems and granting them access back to their systems.

Unlike a ransomware attack, a ransom DDoS attack does not encrypt a company's systems; it aims to knock them offline if the ransom is not paid. What makes ransom DDoS attacks even more dangerous is that they do not require the attacker to gain access to a business's internal systems to execute the attack. However, with a strong DDoS protection strategy in place, a ransom DDoS attack has little to no effect on businesses.

Ransomware and ransom DDoS threats are impacting most industries across the globe — the financial industry, transportation, oil and gas, consumer goods, and even education and healthcare.

Entities claiming to be ‘Fancy Lazarus’, ‘Fancy Bear’, ‘Lazarus Group’, and ‘REvil’ are once again launching ransomware and ransom-DDoS attacks against organizations’ websites and network infrastructure unless a ransom is paid before a given deadline. In the case of DDoS threats, prior to the ransom note, a small DDoS attack is usually launched as a form of demonstration. The demonstration attack is typically over UDP, lasting roughly 30-120 minutes.

The ransom note is typically sent to the common group email aliases of the company that are publicly available online such as noc@, support@, help@, legal@, abuse@, etc. In several cases, it has ended up in spam. In other cases, we’ve seen employees disregard the ransom note as spam, increasing the organization’s response time which resulted in further damage to their online properties.

Cloudflare’s recommendation for organizations that receive a threat or ransom note:

1. **Do not panic, and we recommend you do not pay the ransom**: Paying ransom only encourages and funds bad actors. There's also no guarantee that you won't be attacked again anyway.
2. **Contact local law enforcement**: Be ready to provide a copy of the ransom letter you received and any other logs or packet captures.
3. **Activate an effective DDoS protection strategy**: Cloud-based DDoS protection can be quickly onboarded in the event of an active threat, and with a team of security experts on your side, risks can be mitigated quickly and effectively.

Here's a short video by Cloudflare CTO, John Graham-Cumming addressing the threat of ransom DDoS attacks.

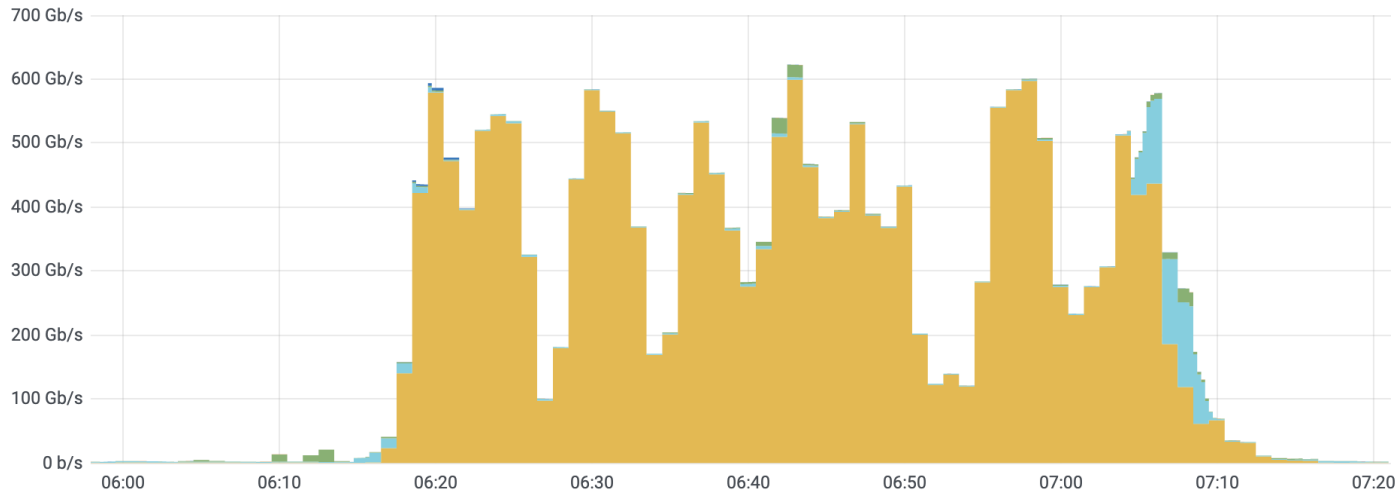
Cloudflare protects Hypixel against a massive DDoS attack campaign

At Cloudflare, our teams have been exceptionally busy this past quarter rapidly onboarding (onto our Magic Transit service) a multitude of new and existing customers that have either received a ransom letter or were under an active DDoS attack.

One such customer is Hypixel Inc, the development studio behind the world's largest Minecraft minigame server. With over 24M total unique logins to date and a world record 216,000+ concurrent players on PC, the Hypixel team works hard to add value to the experience of millions of players across the globe.

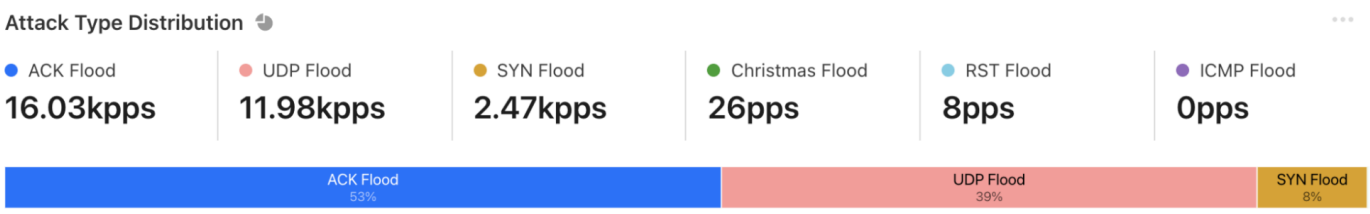
The gaming industry is often subject to some of the largest volumetric DDoS attacks — and as a marquee brand, Hypixel attracts more than its fair share. Uptime and high performance are fundamental to the functioning of Hypixel's servers. Any perceived downtime or noticeable lag could result in an exodus of gamers.

When Hypixel was under a massive DDoS attack campaign, they turned to Cloudflare to extend their services with Cloudflare to include Magic Transit, Cloudflare's BGP-based DDoS protection service for network infrastructure. After rapidly onboarding them overnight, Cloudflare was automatically able to detect and mitigate DDoS attacks targeting their network — several of which were well over 620 Gbps. The DDoS attack comprised mostly TCP floods and UDP amplification attacks. In the graph, the various colors represent the multiple Cloudflare systems that contribute to detecting and mitigating the multi-vector attack — emphasising the value of our multi-layered DDoS approach.



Even as attack patterns changed in real-time, Magic Transit shielded Hypixel's network. In fact, because all their clean traffic routed over Cloudflare's high performing low-latency network, Hypixel's users noticed no change in gamer experience — even during an active volumetric DDoS attack.

During the attack campaign, Cloudflare automatically detected and mitigated over 5,000 DDoS attacks: 53% were ACK floods, 39% were UDP-based attacks and 8% SYN floods.



> *"We had several attacks of well over 620 Gbps with no impact at all on our players. Their gaming experience remained uninterrupted and fast, thanks to Cloudflare Magic Transit."*
> - **Simon Collins-Laflamme, CEO, Hypixel Inc.**

Hypixel's journey with Cloudflare began with them employing Cloudflare Spectrum to help protect their gaming infrastructure against DDoS attacks. As their user base grew, they adopted additional Cloudflare products to bolster the robustness and resilience of all of their critical infrastructure. Today, they use multiple Cloudflare products including CDN, Rate Limiting, Spectrum, Argo Smart Routing, and Load Balancing to build and secure infrastructure that provides gamers around the world the real-time gaming experiences they need.

Get holistic protection against cyber attacks of any kind

DDoS attacks constitute just one facet of the many cyber threats organizations are facing today. As businesses shift to a Zero Trust approach, network and security buyers will face larger threats related to network access, and a continued surge in the frequency and sophistication of bot-related and ransomware attacks.

A key design tenet while building products at Cloudflare is integration. Cloudflare One is a solution that uses a Zero Trust security model to provide companies a better way to protect devices, data, and applications — and is deeply integrated with our existing platform of security and DDoS solutions.

In fact, Cloudflare offers an integrated solution that comprises an all-star cast featuring the following to name a few:

- **DDoS**: LEADER in Forrester Wave™ for DDoS Mitigation Solutions, Q1 2021[1]

- **WAF**: Cloudflare is a CHALLENGER in the 2020 Gartner Magic Quadrant for Web Application Firewall (receiving the highest placement in the 'Ability to Execute')[2]
- **Zero Trust**: Cloudflare is a LEADER in the Omdia Market Radar: Zero-Trust Access Report, 2020[3]
- **Web protection**: Innovation leader in the Global Holistic Web Protection Market for 2020 by Frost & Sullivan[4]

Cloudflare's global (and growing) network is uniquely positioned to deliver DDoS protection and other security, performance, and reliability services with unparalleled scale, speed, and smarts.

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

———

[1]Forrester Wave™: DDoS Mitigation Solutions, Q1 2021, Forrester Research, Inc., March 3, 2021. Access the report at https://www.cloudflare.com/forrester-wave-ddos-mitigation-2021/
[2]Gartner, "Magic Quadrant for Web Application Firewalls", Analyst(s): Jeremy D'Hoinne, Adam Hils, John Watts, Rajpreet Kaur, October 19, 2020. https://www.cloudflare.com/gartner-mq-waf-2020/
[3] https://www.cloudflare.com/lp/omdia-zero-trust
[4]https://www.cloudflare.com/lp/frost-radar-holistic-web/

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 Cloudflare Radar Ransom DDoS