DDoS Attack Trends for Q3 2021

blog.cloudflare.com/ddos-attack-trends-for-2021-q3

4 november 2021

04-11-2021

-
  Vivek Ganti
-
  Omer Yoachimik

The third quarter of 2021 was a busy quarter for DDoS attackers. Cloudflare observed and mitigated record-setting HTTP DDoS attacks, terabit-strong network-layer attacks, one of the largest botnets ever deployed (Meris), and more recently, ransom DDoS attacks on voice over IP (VoIP) service providers and their network infrastructure around the world.

Here's a summary of the trends observed in Q3 '21:

Application-layer (L7) DDoS attack trends:

- For the second consecutive quarter in 2021, US-based companies were the most targeted in the world.
- For the first time in 2021, attacks on UK-based and Canada-based companies skyrocketed, making them the second and third most targeted countries, respectively.

- Attacks on Computer Software, Gaming/ Gambling, IT, and Internet companies increased by an average of 573% compared to the previous quarter.
- Meris, one of the most powerful botnets in history, aided in launching DDoS campaigns across various industries and countries.

Network-layer (L3/4) DDoS attack trends:

- DDoS attacks increased by 44% worldwide compared to the previous quarter.
- The Middle East and Africa recorded the largest average attack increase of approximately 80%.
- Morocco recorded the highest DDoS activity in the third quarter globally — three out of every 100 packets were part of a DDoS attack.
- While SYN and RST attacks remain the dominant attack method used by attackers, Cloudflare observed a surge in DTLS amplification attacks — recording a 3,549% increase QoQ.
- Attackers targeted (and continue to target going into the fourth quarter this year) VoIP service providers with massive DDoS attack campaigns in attempts to bring SIP infrastructure down.

Note on avoiding data biases: When we analyze attack trends, we calculate the “DDoS activity” rate, which is the percentage of attack traffic of the total traffic (attack + clean). When reporting application- and network-layer DDoS attack trends, we use this metric, which allows us to normalize the data points and avoid biases toward, for example, a larger Cloudflare data center that naturally handles more traffic and therefore also, possibly, more attacks compared to a smaller Cloudflare data center located elsewhere.

Application-layer DDoS attacks

Application-layer DDoS attacks, specifically HTTP DDoS attacks, are attacks that usually aim to disrupt a web 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 and — in some cases — crash, resulting in degraded performance or an outage for legitimate users.

Q3 ‘21 was the quarter of Meris — one of the most powerful botnets deployed to launch some of the largest HTTP DDoS attacks in history.

This past quarter, we observed one of the largest recorded HTTP attacks — 17.2M rps (requests per second) — targeting a customer in the financial services industry. One of the most powerful botnets ever observed, called Meris, is known to be deployed in launching these attacks.

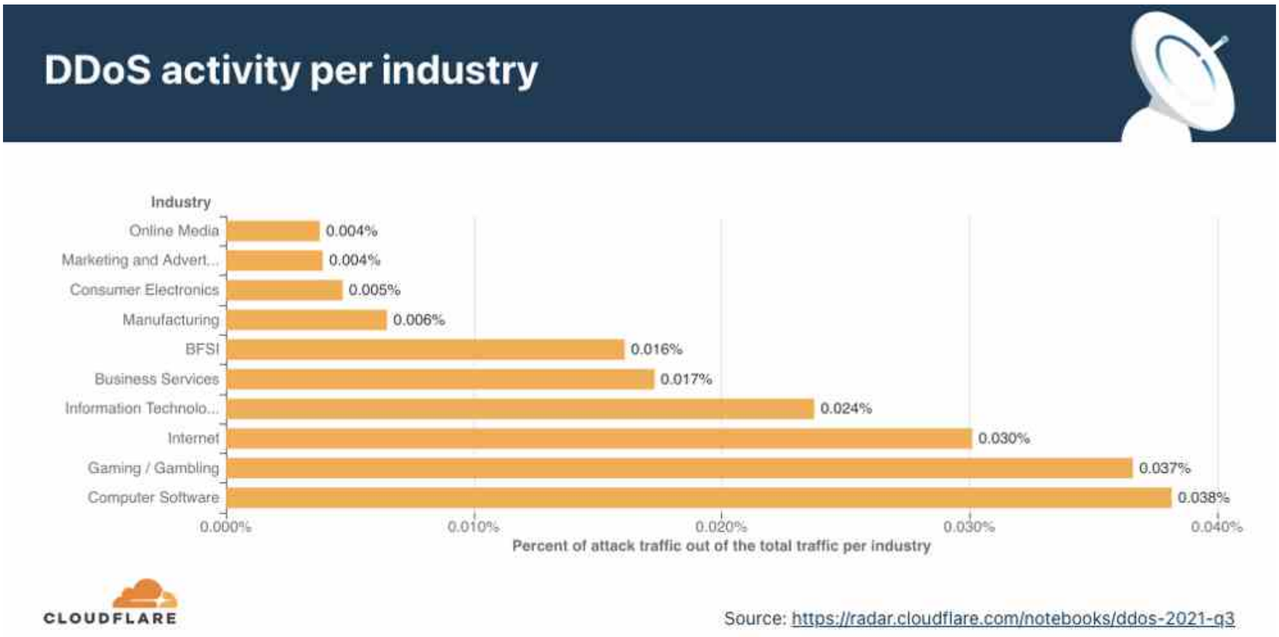
Meris (Latvian for plague) is a botnet behind recent DDoS attacks that have targeted networks or organizations around the world. The Meris botnet infected routers and other networking equipment manufactured by the Latvian company MikroTik. According to MikroTik’s blog, a vulnerability in the MikroTik RouterOS (that was patched after its detection back in 2018) was exploited in still unpatched devices to build a botnet and launch coordinated DDoS attacks by bad actors.

Similar to the Mirai botnet of 2016, Meris is one of the most powerful botnets recorded. While Mirai infected IoT devices with low computational power such as smart cameras, Meris is a growing swarm of networking infrastructure (such as routers and switches) with significantly higher processing power and data transfer capabilities than IoT devices — making them much more potent in causing harm at a larger scale. Be that as it may, Meris is an example of how the attack volume doesn’t necessarily guarantee damage to the target. As far as we know, Meris, despite its strength, was not able to cause significant impact or Internet outages. On the other hand, by tactically targeting the DYN DNS service in 2016, Mirai succeeded in causing significant Internet disruptions.

Application-layer DDoS attacks by industry

The tech and gaming industries were the most targeted industries in Q3 ‘21.

When we break down the application-layer attacks targeted by industry, Computer Software companies topped the charts. The Gaming/Gambling industry, also known to be regular targets of online attacks, was a close second, followed by the Internet and IT industries.



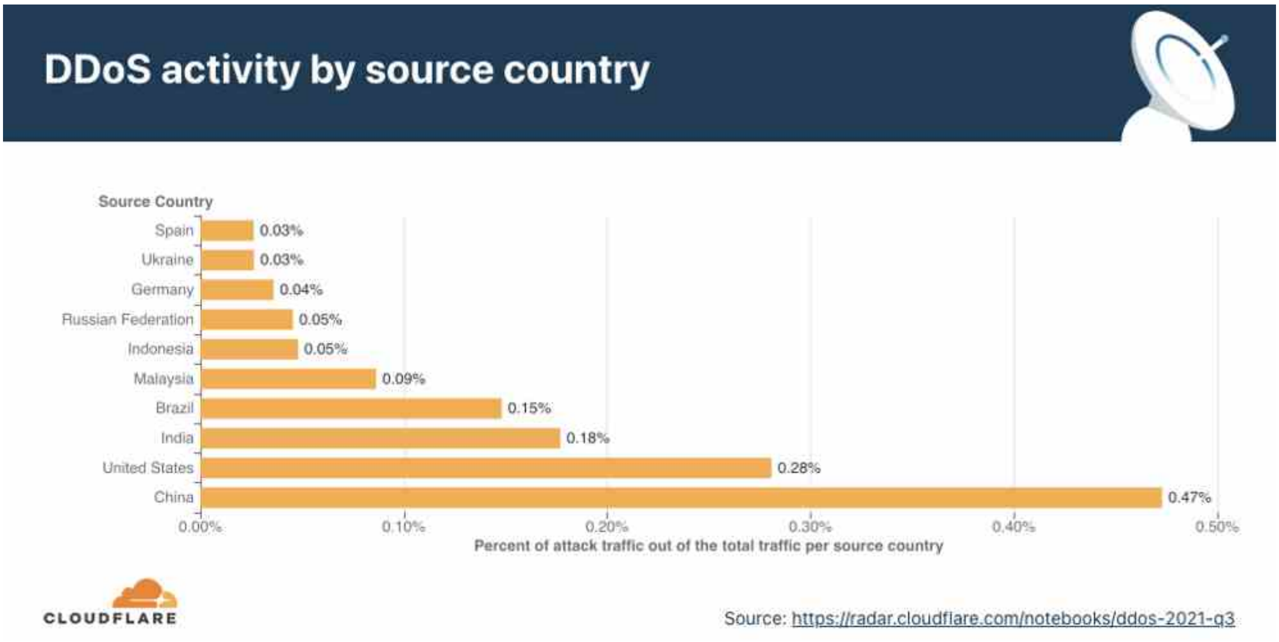
Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Application-layer DDoS attacks by source country

To understand the origin of the HTTP attacks, we look at the geolocation of the source IP address belonging to the client that generated 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 usually indicates the presence of botnets operating from within.

In the third quarter of 2021, most attacks originated from devices/servers in China, the United States, and India. While China remains in first place, the number of attacks originating from Chinese IPs actually decreased by 30% compared to the previous quarter. Almost one out of every 200 HTTP requests that originated from China was part of an HTTP DDoS attack.

Additionally, attacks from Brazil and Germany shrank by 38% compared to the previous quarter. Attacks originating from the US and Malaysia reduced by 40% and 45%, respectively.

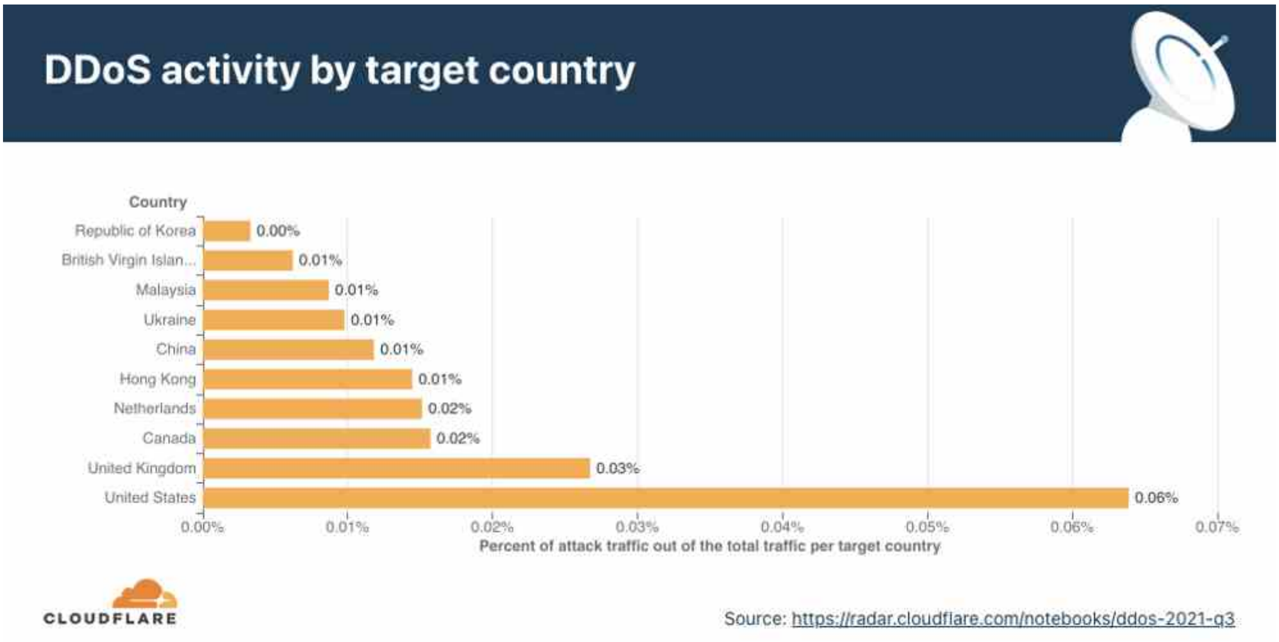


Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Application-layer DDoS attacks by target country

In order to identify which countries are targeted the most by L7 attacks, we break down the DDoS activity by our customers' billing countries.

For the second consecutive time this year, organizations in the United States were targeted the most by L7 DDoS attacks in the world, followed by those in the UK and Canada.



Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Network-layer DDoS attacks

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

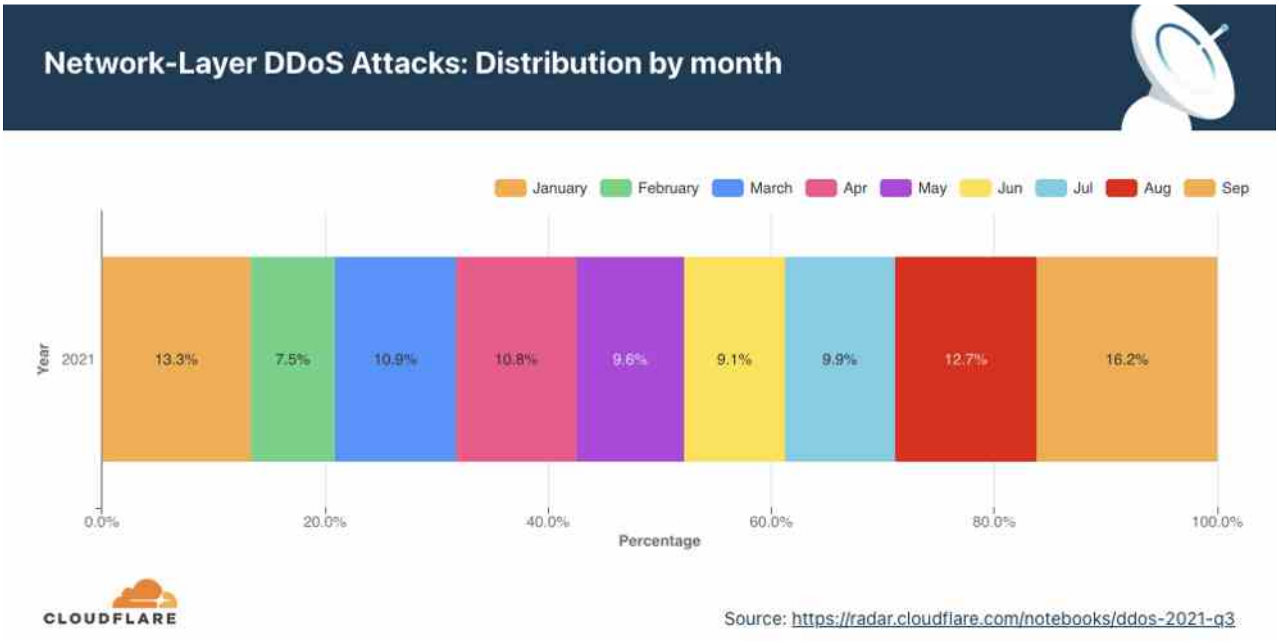
Mirai-variant botnet strikes with a force of 1.2 Tbps.

Q3 ‘21 was also the quarter when the infamous Mirai made a resurgence. A Mirai-variant botnet launched over a dozen UDP- and TCP-based DDoS attacks that peaked multiple times above 1 Tbps, with a max peak of approximately 1.2 Tbps. These network-layer attacks targeted Cloudflare customers on the Magic Transit and Spectrum services. One of these targets was a major APAC-based Internet services, telecommunications, and hosting provider and the other was a gaming company. In all cases, the attacks were automatically detected and mitigated without human intervention.

Network-layer DDoS attacks by month

September was, by far, the busiest month for attackers this year.

Q3 ‘21 accounted for more than 38% of all attacks this year. September was the busiest month for attackers so far in 2021 — accounting for over 16% of all attacks this year.



Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

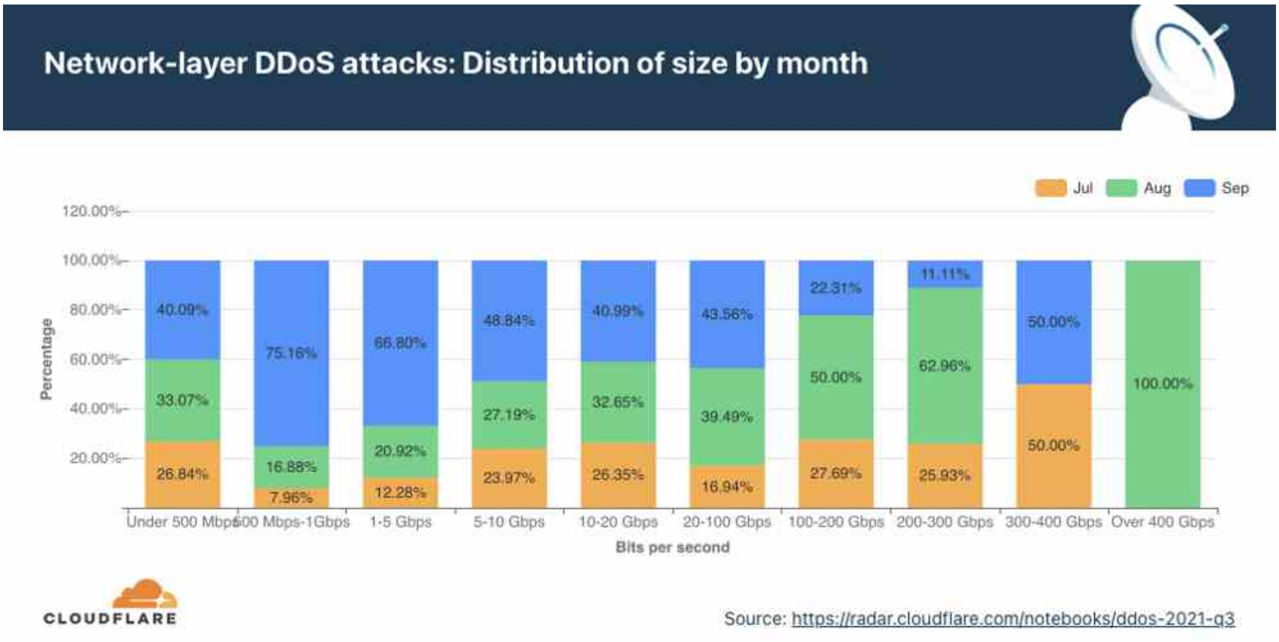
Network-layer DDoS attacks by attack rate

Most attacks are ‘small’ in size, but the number of larger attacks continues to rise.

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, terabits per second or gigabits per second). Another is the number of packets it delivers, measured as the packet rate (specifically, millions of packets per second).

Attacks with high bit rates attempt to cause a denial-of-service event by clogging the Internet link, while attacks with high packet rates attempt to overwhelm the servers, routers, or other in-line hardware appliances. Appliances dedicate a certain amount of memory and computation power to process each packet. Therefore, by bombarding it with many packets, the appliance can be left with no further processing resources. In such a case, packets are “dropped,” i.e., the appliance is unable to process them. For users, this results in service disruptions and denial of service.

The distribution of attacks by their size (in bit rate) and month is shown below. Interestingly enough, all attacks over 400 Gbps took place in August, including some of the largest attacks we have seen; multiple attacks peaked above 1 Tbps and reached as high as 1.2 Tbps.

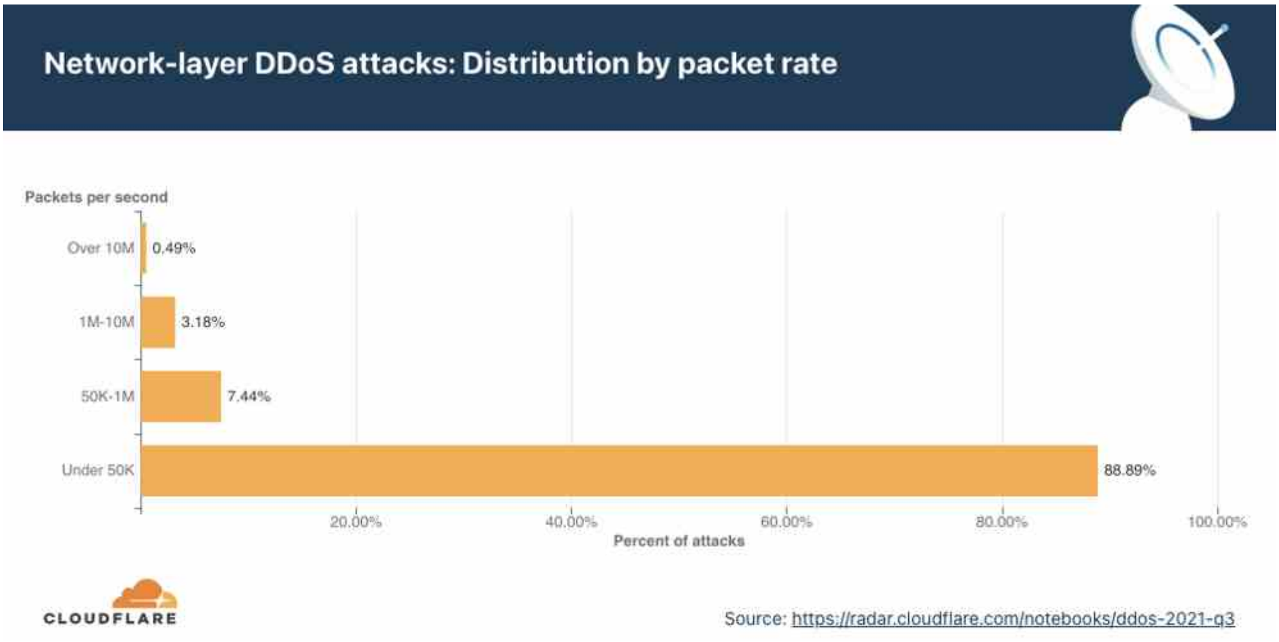


Network-layer DDoS attacks: Distribution of size by month

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Packet rate

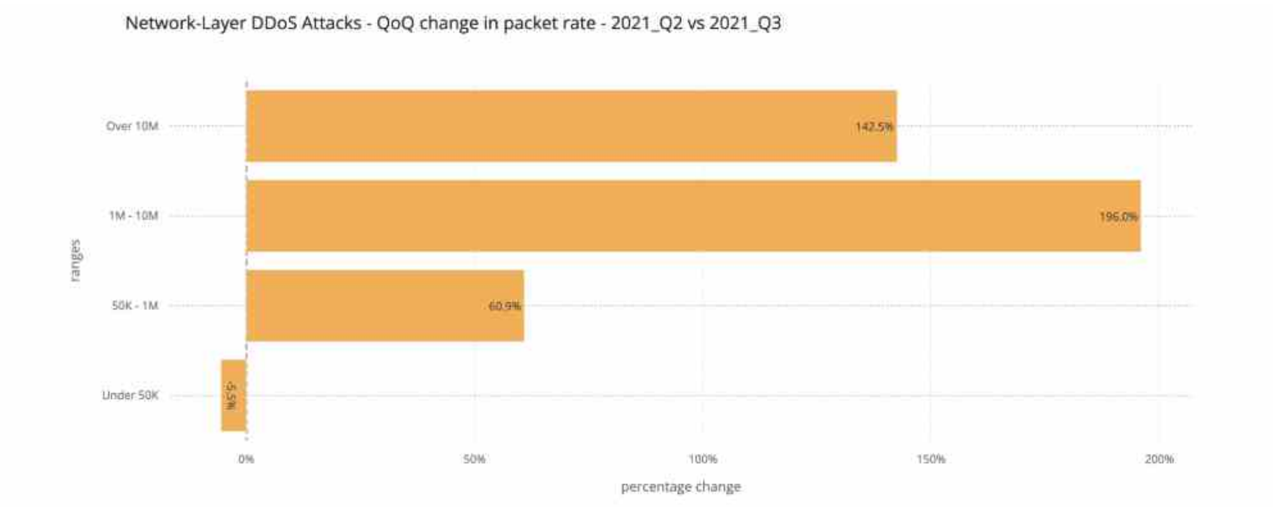
As seen in previous quarters, the majority of attacks observed in Q3 ‘21 were relatively small in size — nearly 89% of all attacks peaked below 50K packets per second (pps). While a majority of attacks are smaller in size, we observed that the number of larger attacks is increasing QoQ — attacks that peaked above 10M pps increased by 142% QoQ.



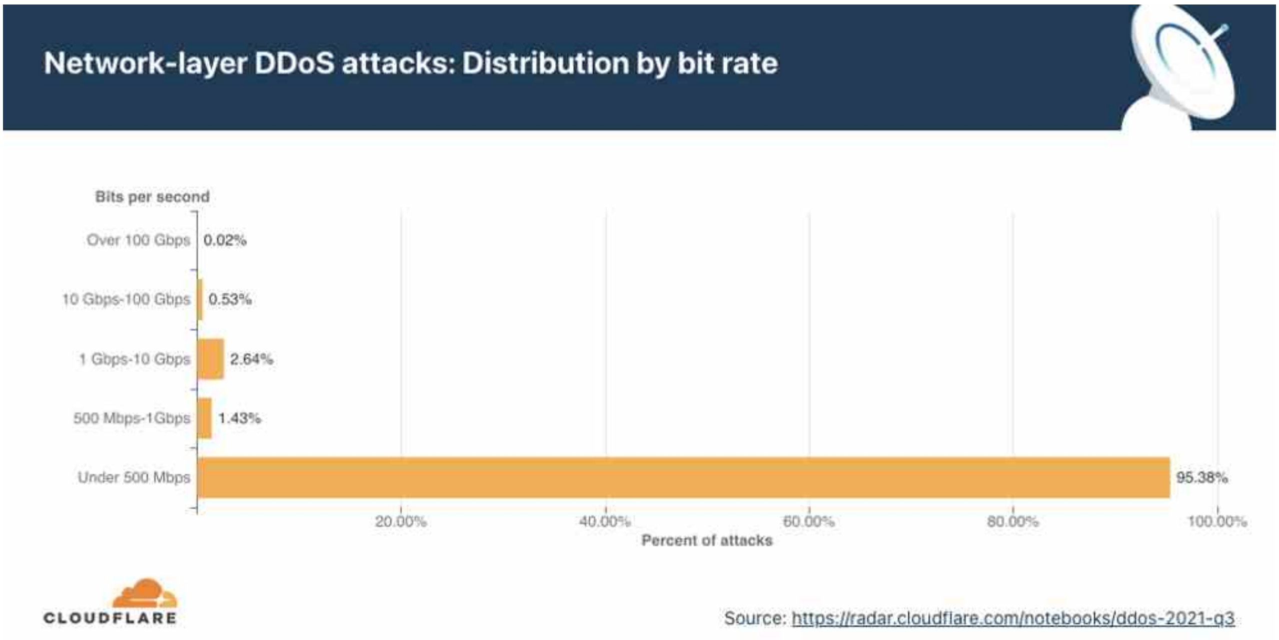
Network-layer DDoS attacks: Distribution by packet rate

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Attacks of packet rates ranging from 1-10 million packets per second increased by 196% compared to the previous quarter. This trend is similar to what we observed the last quarter as well, suggesting that larger attacks are increasing.


Network-Layer DDoS Attacks - QoQ change in packet rate - 2021_Q2 vs 2021_Q3

Bit rate
From the bit rate perspective, a similar trend was observed — a total of 95.4% of all attacks peaked below 500 Mbps.

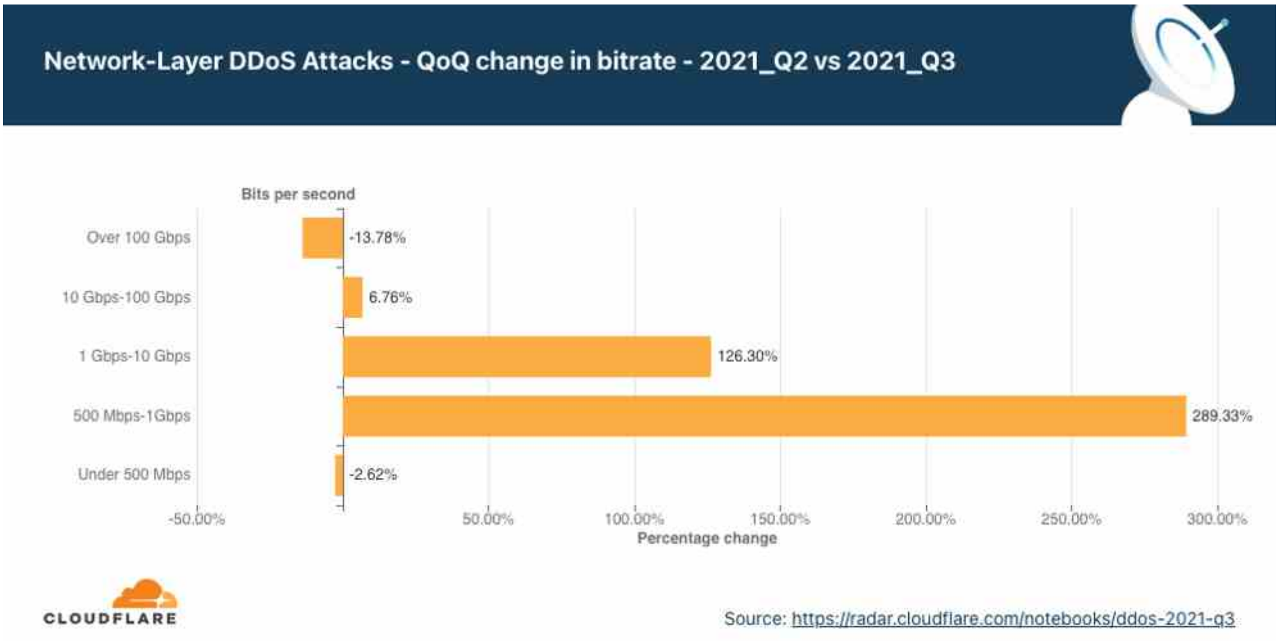

Network-layer DDoS attacks: Distribution by bit rate

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

QoQ data shows that the number of attacks of sizes ranging from 500 Mbps to 10 Gbps saw massive increases of 126% to 289% compared to the previous quarter. Attacks over 100 Gbps decreased by nearly 14%.

The number of larger bitrate attacks increased QoQ (with the one exception being attacks over 100 Gbps, which decreased by nearly 14% QoQ). In particular, attacks ranging from 500 Mbps to 1 Gbps saw a surge of 289% QoQ and those ranging from 1 Gbps to 100 Gbps surged by 126%.

This trend once again illustrates that, while (in general) a majority of the attacks are indeed smaller, the number of “larger” attacks is increasing. This suggests that more attackers are garnering more resources to launch larger attacks.



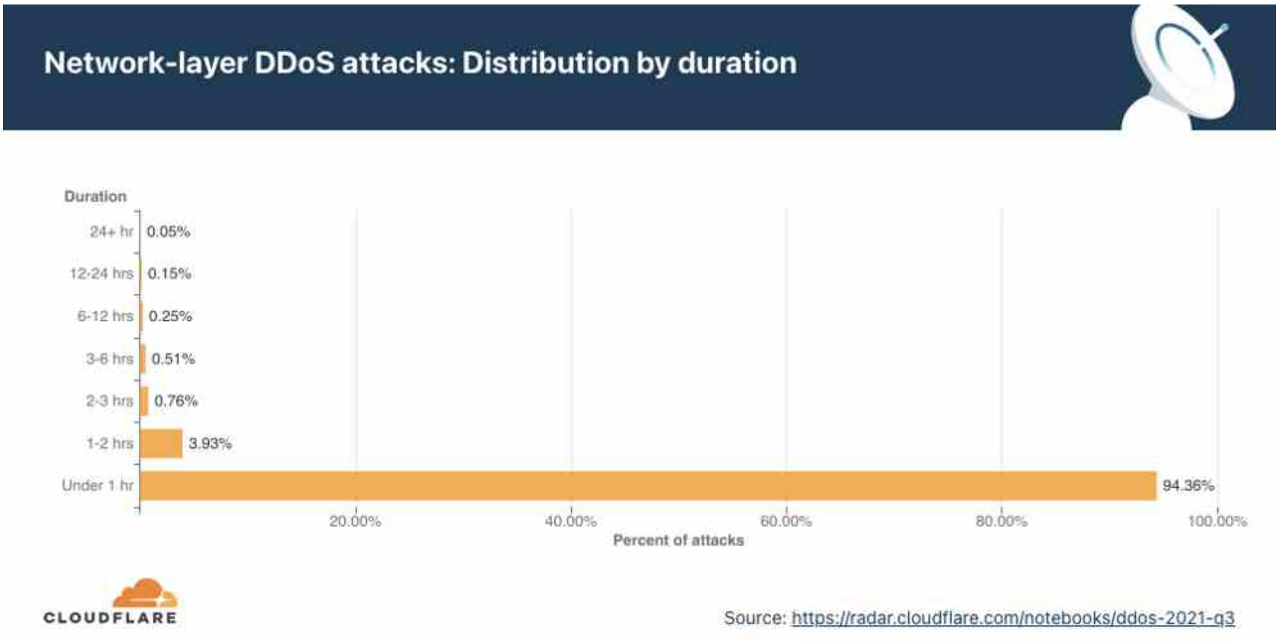
Network-Layer DDoS Attacks - QoQ change in bitrate - 2021_Q2 vs 2021_Q3

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Network-layer DDoS attacks by duration

Most attacks remain under one hour in duration, reiterating the need for automated always-on DDoS mitigation solutions.

We measure the duration of an attack by recording the difference between when it is first detected by our systems as an attack and the last packet we see with that attack signature. As in previous quarters, most of the attacks are short-lived. To be specific, 94.4% of all DDoS attacks lasted less than an hour. On the other end of the axis, attacks over 6 hours accounted for less than 0.4% in Q3 ‘21, and we did see a QoQ increase of 165% in attacks ranging 1-2 hours. Be that as it may, a longer attack does not necessarily mean a more dangerous one.



Network-layer DDoS attacks: Distribution by duration

Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Short attacks can easily go undetected, especially burst attacks that, within seconds, bombard a target with a significant number of packets, bytes, or requests. In this case, DDoS protection services that rely on manual mitigation by security analysis have no chance in mitigating the attack in time. They can only learn from it in their post-attack analysis, then deploy a new rule that filters the attack fingerprint and hope to catch it next time. Similarly, using an “on-demand” service, where the security team will redirect traffic to a DDoS provider during the attack, is also inefficient because the attack will already be over before the traffic routes to the on-demand DDoS provider.

Cloudflare recommends that companies use automated, always-on DDoS protection services that analyze traffic and apply real-time fingerprinting fast enough to block the short-lived attacks. Cloudflare analyzes traffic out-of-path, ensuring that DDoS mitigation does not add any latency to legitimate traffic, even in always-on deployments. Once an attack is identified, our autonomous edge DDoS protection system (dosd) generates and applies a dynamically crafted rule with a real-time signature. Pre-configured firewall rules comprising allow/deny lists for known traffic patterns take effect immediately.

Attack vectors

SYN floods remain attackers’ favorite method of attack, while attacks over DTLS saw a massive surge — 3,549% QoQ.

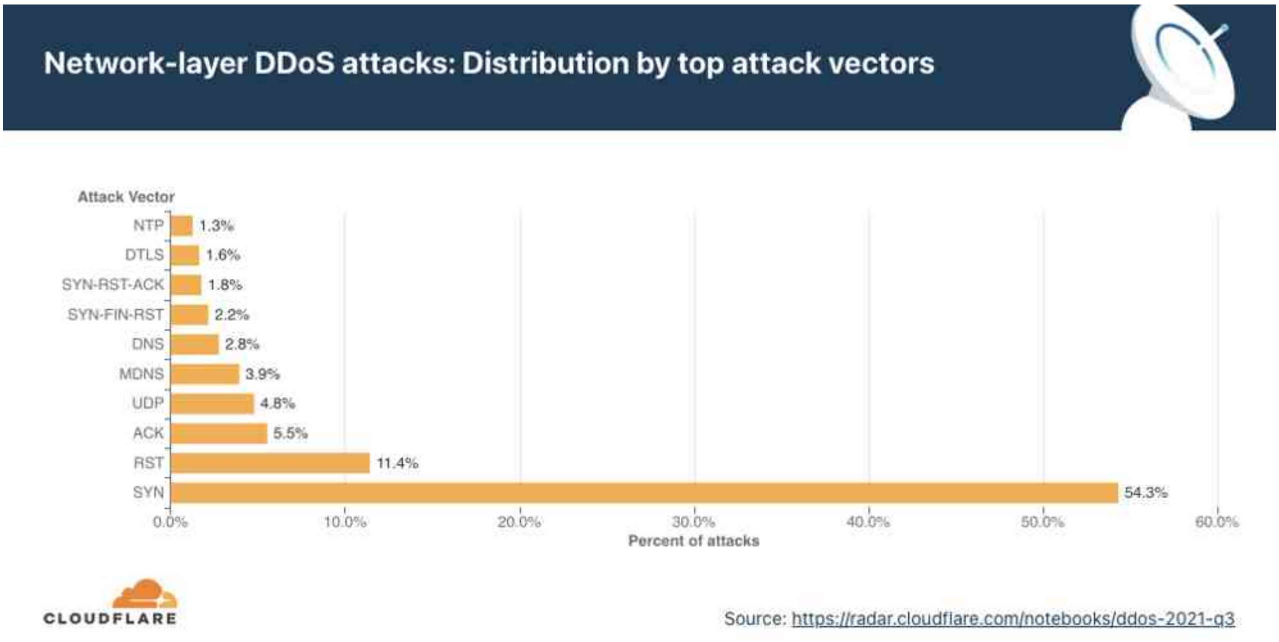
An attack vector is the term used to describe the method that the attacker utilizes in their attempt to cause a denial-of-service event.

As observed in previous quarters, attacks utilizing SYN floods remain the most popular method used by attackers.

A SYN flood attack is a DDoS attack that works by exploiting the very foundation of the TCP protocol — the stateful TCP connection between a client and a server as a part of the 3-way TCP handshake. As a part of the 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 server 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 server’s memory, the server is unable to allocate further memory for legitimate clients, causing the server to crash or preventing it from handling legitimate client connections, i.e., a denial-of-service event.

More than half of all attacks observed over our network were SYN floods. This was followed by RST, ACK, and UDP floods.

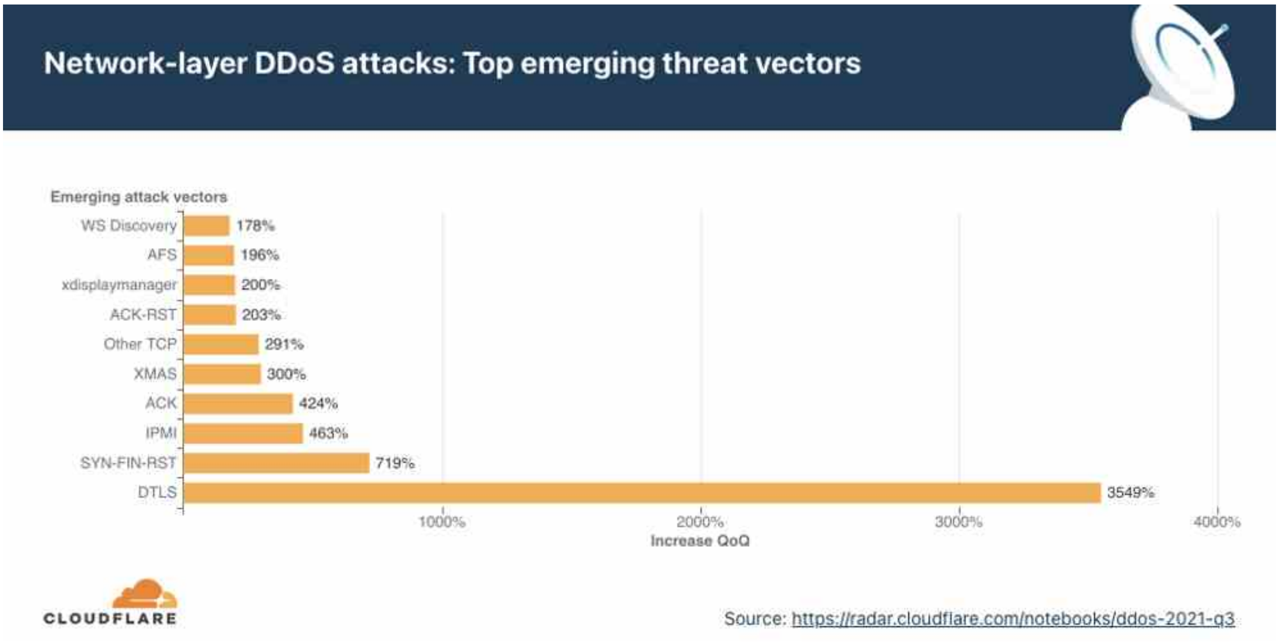


Emerging threats

While SYN and RST floods remain popular overall, when we look at emerging attack vectors — which helps us understand what new vectors attackers are deploying to launch attacks — we observed a massive spike in DTLS amplification attacks. DTLS floods increased by 3,549% QoQ.

Datagram Transport Layer Security (DTLS) is a protocol similar to Transport Layer Security (TLS) designed to provide similar security guarantees to connectionless datagram-based applications to prevent message forgery, eavesdropping, or tampering. DTLS, being connectionless, is specifically useful for establishing VPN connections, without the TCP meltdown problem. The application is responsible for reordering and other connection properties.

Just as with most UDP-based protocols, DTLS is spoofable and being used by attackers to generate reflection amplification attacks to overwhelm network gateways.



Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

Network-layer DDoS attacks by country

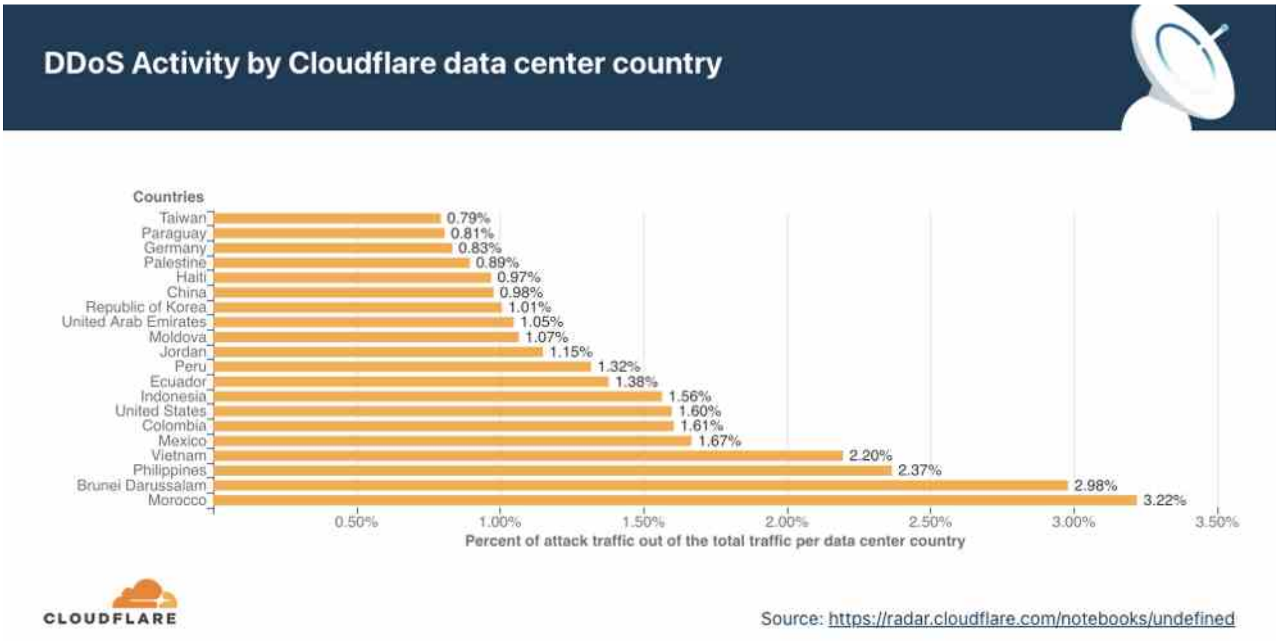
While Morocco topped the charts in terms of the highest network attack rate observed, Asian countries closely followed.

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 the Cloudflare data center in which the attack was observed. We are able to achieve geographical accuracy in our report because we have data centers in over 250 cities around the world.

Worldwide

DDoS Activity by Cloudflare data center country



Source: https://radar.cloudflare.com/notebooks/undefined

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

A note on recent attacks on voice over-IP service providers — and ransom DDoS attacks

We recently reported and provided an update on the surge in DDoS attacks on VoIP service providers — some of who have also received ransom threats. As of early Q4 ‘21, this attack campaign is still ongoing and current. At Cloudflare, we continue to onboard VoIP service providers and shield their applications and networks against attacks.

HTTP attacks against API gateways and the corporate websites of the providers have been combined with network-layer and transport-layer attacks against VoIP infrastructures.

Examples include:

1. **TCP floods targeting stateful firewalls:** These are being used in “trial-and-error” type attacks. They are not very effective against telephony infrastructure specifically (because it is mostly UDP) but very effective at overwhelming stateful firewalls.
2. **UDP floods targeting SIP infrastructure:** Floods of UDP traffic that have no well-known fingerprint, aimed at critical VoIP services. Generic floods like this may look like legitimate traffic to unsophisticated filtering systems.
3. **UDP reflection targeting SIP infrastructure:** These methods, when targeted at SIP or RTP services, can easily overwhelm Session Border Controllers (SBCs) and other telephony infrastructure. The attacker seems to learn enough about the target’s infrastructure to target such services with high precision.
4. **SIP protocol-specific attacks:** Attacks at the application layer are of particular concern because of the higher resource cost of generating application errors versus filtering on network devices.

Organizations also continue to receive ransom notes that threaten attacks in exchange for bitcoin. Ransomware and ransom DDoS attacks, for the fourth consecutive quarter, continue to be a germane threat to organizations all over the world.

Cloudflare products close off several threat vectors that can lead to a ransomware infection and ransom DDoS attacks:

- Cloudflare DNS filtering blocks unsafe websites.
- Cloudflare Browser Isolation prevents drive-by downloads and other browser-based attacks.
- A Zero Trust architecture can help prevent ransomware from spreading within a network.
- Magic Transit protects organizations’ networks against DDoS attacks using BGP route redistribution — without impacting latency.

Helping build a better Internet

Cloudflare was founded on the mission to help build a better Internet. And part of that mission is to build an Internet 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. In 2017, we announced unmetered DDoS protection for free — as part of every Cloudflare service and plan, including the Free plan — to make sure every organization can stay protected and available. Organizations big and small have joined Cloudflare over the past several years to ensure their websites, applications, and networks are secure from DDoS attacks, and remain fast and reliable.

But cyberattacks come in various forms, not just DDoS attacks. Malicious bots, ransomware attacks, email phishing, and VPN / remote access hacks are some many attacks that continue to plague organizations of all sizes globally. These attacks target websites, APIs, applications, and entire networks — which form the lifeblood of any online business. That is why the Cloudflare security portfolio accounts for everything and everyone connected to the Internet.