CLOUDFLARE

THREAT REPORT

DDoS Threat Landscape Report

DDoS Trends from Q3 2022

Content

Executive Summary

Welcome to Cloudflare's quarterly distributed denial-of-service (DDoS) report. This report uncovers insights and trends about the DDoS threat landscape observed across the global Cloudflare network from July to September of 2022.

During this time period, we saw an increase in the number of multi-terabit volumetric attacks, the largest attack we've seen to date (in terms of bitrate), and a doubling of network-layer DDoS attacks year-over-year. We also saw the Mirai botnet gain momentum, with a 405% increase in network-layer DDoS attacks attributed to the botnet and its variants. The gaming and gambling industries were most targeted by network-layer attacks — with almost one out of every five gaming and gambling-oriented IP packets ingested by Cloudflare attributable to DDoS attacks. This represents a startling 381% increase quarter-over-quarter.

In the sections below, we will outline general DDoS attack trends before breaking down application-layer, network-layer, and ransom DDoS attack insights. We also explore where DDoS attacks have been observed, share patterns in attack rates and durations, and dive deeper into attack vectors and emerging threats. Finally, we provide guidance on how to proactively harden your security to better prepare for current and emerging DDoS threats.

An interactive version of this report is also available on Cloudflare Radar.

Report Highlights

① General DDoS attack trends

Overall this quarter, we've seen:

- An increase in DDoS attacks compared to last year
- Longer-lasting volumetric attacks, including a spike in attacks generated by the Mirai botnet and its variants
- Surges in attacks targeting Taiwan and Japan

② Ransom DDoS attack insights

- 15% of Cloudflare customers that responded to our survey reported being targeted by HTTP DDoS attacks accompanied by a threat or a ransom note
- Reported ransom DDoS attacks increased 15% quarter-over-quarter and 67% year-over-year
- In September 2022, almost one out of every four respondents reported receiving a ransom DDoS attack or threat — the most reported ransom DDoS attacks in a single month this year so far

③ Application-layer DDoS attack insights

- HTTP DDoS attacks increased by 111% year-over-year, but decreased by 10% quarter-over-quarter
- HTTP DDoS attacks targeting Taiwan increased by 200% quarter-over-quarter; attacks targeting Japan increased by 105% quarter-over-quarter
- Reports of ransom DDoS attacks increased by 67% year-over-year and 15% quarter-over-quarter

④ Network-layer DDoS attack insights

- L3/4 DDoS attacks increased by 97% year-over-year and 24% quarter-over-quarter
- L3/4 DDoS attacks by Mirai botnets increased by 405% quarter-over-quarter
- The gaming and gambling industries were the most targeted by L3/4 DDoS attacks, including a massive 2.5 Tbps attack

A note on how we measure DDoS attacks observed over our network

This report is based on DDoS attacks that were automatically detected and mitigated by Cloudflare's DDoS Protection systems. To learn more about how it works, check out this deep-dive blog post.

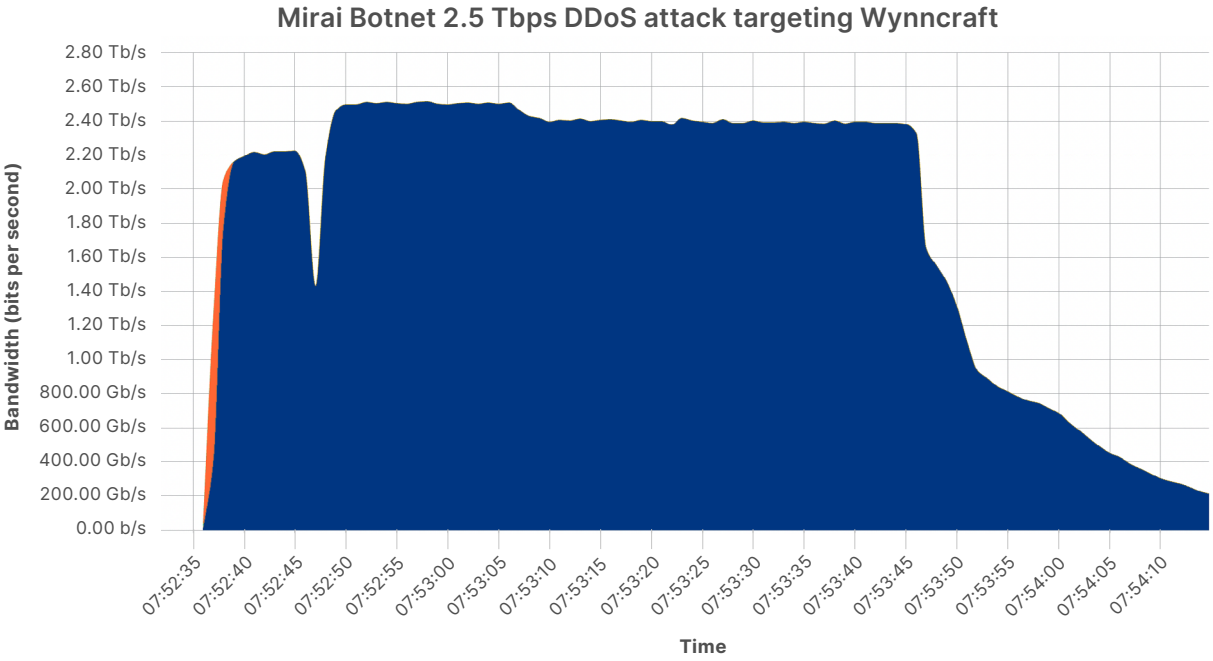
To analyze attack trends, we calculate the "DDoS activity" rate, which is either the percentage of attack traffic out of the total traffic (attack + clean) observed over our global network, or in a specific location, or in a specific category (e.g., industry or billing country). Measuring the percentages allows us to normalize data points and avoid biases reflected in absolute numbers towards, for example, a Cloudflare data center that receives more total traffic and likely, also more attacks.

Report

Largest attack to date

Multi-terabit DDoS attacks have become increasingly frequent. In the third quarter of 2022, Cloudflare automatically detected and mitigated multiple attacks that exceeded one Terabit per second (Tbps). The largest attack was a 2.5 Tbps DDoS attack launched by a Mirai botnet variant, aimed at the Minecraft server Wynncraft. This is the largest attack we've seen to date from a bitrate perspective.

It was a multi-vector attack consisting of UDP and TCP floods. Wynncraft is a massive multiplayer online role-playing game that utilizes a Minecraft server where hundreds and thousands of users play on the same server simultaneously. Cloudflare mitigated the attack successfully, which meant there was no impact on the customer or the customer's end user experience despite its size and complexity.



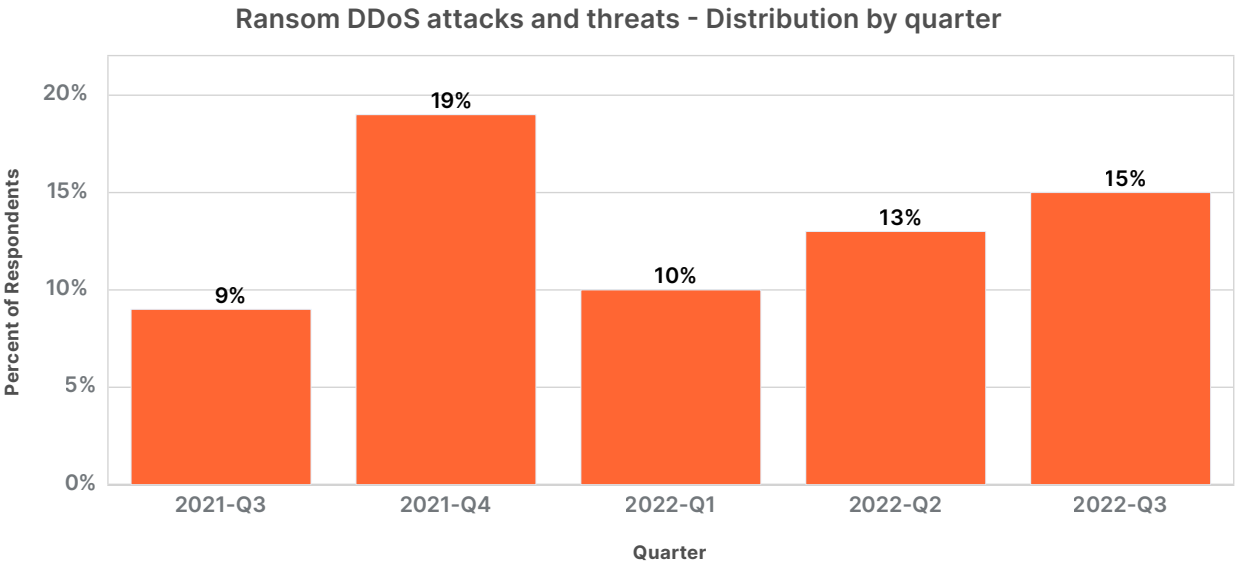
	Mean	Last	Max
l4drop	1.84 Tb/s	207.57 Gb/s	2.52 Tb/s
iptables	286.04 Gb/s	972.80 Mb/s	843.30 Gb/s

Ransom attacks

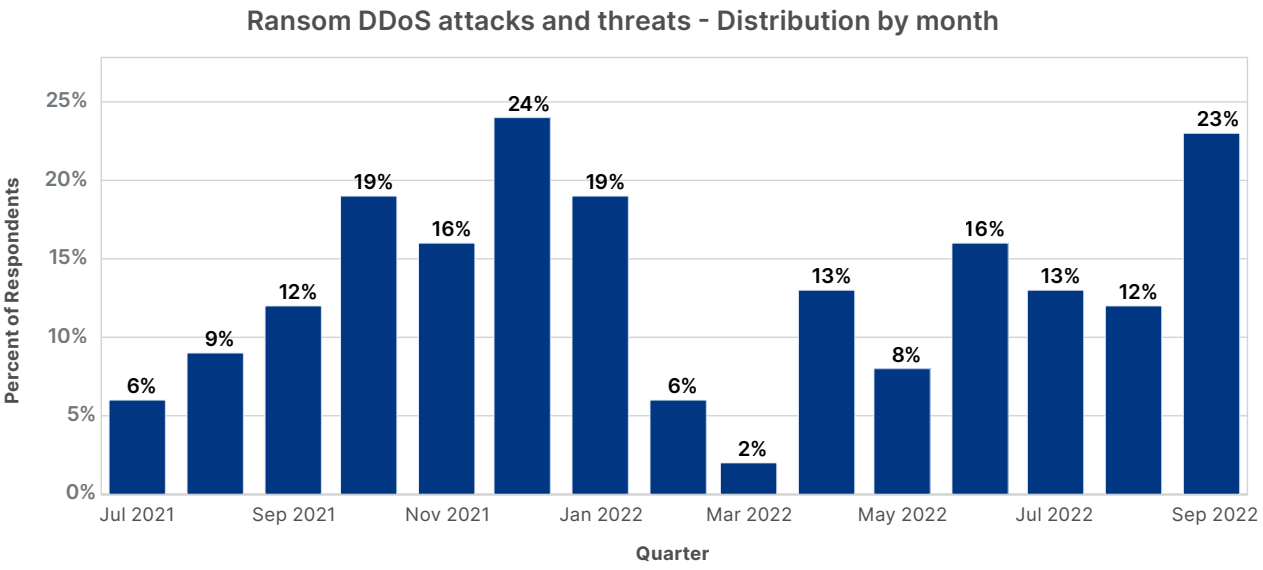
In ransom DDoS attacks, the attacker demands a ransom payment — usually in the form of Bitcoin — to stop/avoid the attack. In the third quarter of 2022, 15% of Cloudflare customers that responded to our survey reported being targeted by HTTP DDoS attacks with an accompanying threat or a ransom note. This represents a 15% increase quarter-over-quarter and 67% increase year-over-year of reported ransom DDoS attacks.

How we calculate Ransom DDoS attack trends

Our systems constantly analyze traffic and automatically apply mitigation when DDoS attacks are detected. Each DDoS'd customer is then prompted with an automated survey to help us better understand the nature of the attack and the success of the mitigation. Cloudflare has been surveying attacked customers for over two years. One of the questions in the survey asks if the customer received a threat or a ransom note demanding payment in exchange to stop the DDoS attack. Over the past year, on average, we collected 174 responses per quarter.
The responses of this survey are used to calculate the percentage of Ransom DDoS attacks.

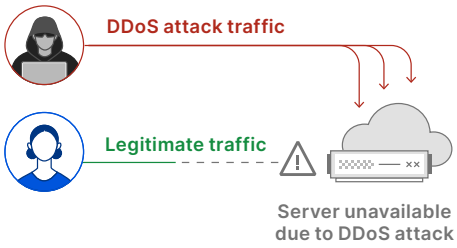


Since June, there has been a steady decline in reports of ransom attacks. However, in September, the reports of ransom attacks spiked again. In the month of September, almost one out of every four respondents reported receiving a ransom DDoS attack or threat — the most active month in 2022 so far.



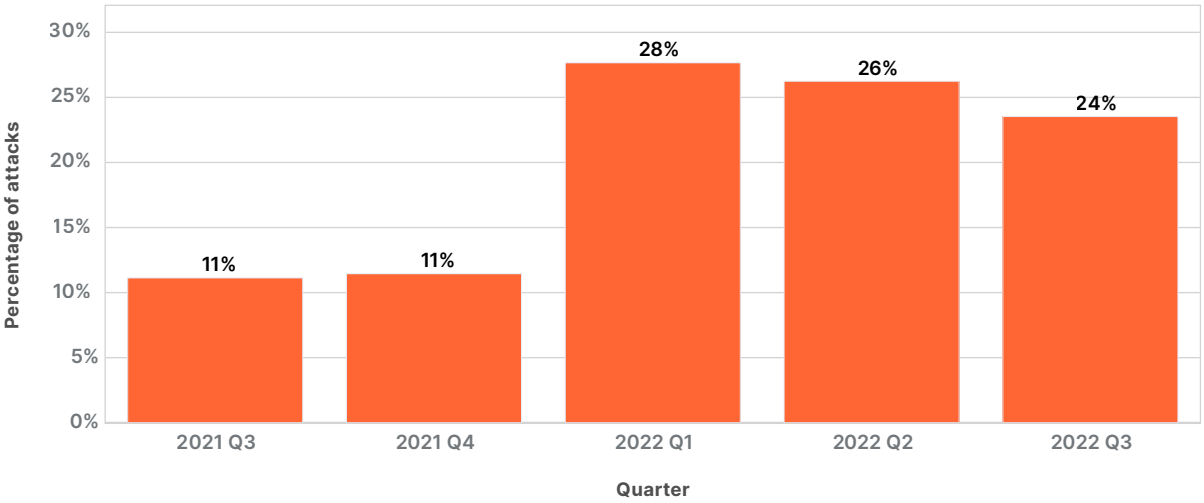
Application-layer DDoS attacks

Application-layer DDoS attacks, specifically HTTP DDoS attacks, typically 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 or crash altogether, resulting in degraded performance or an outage for legitimate users.

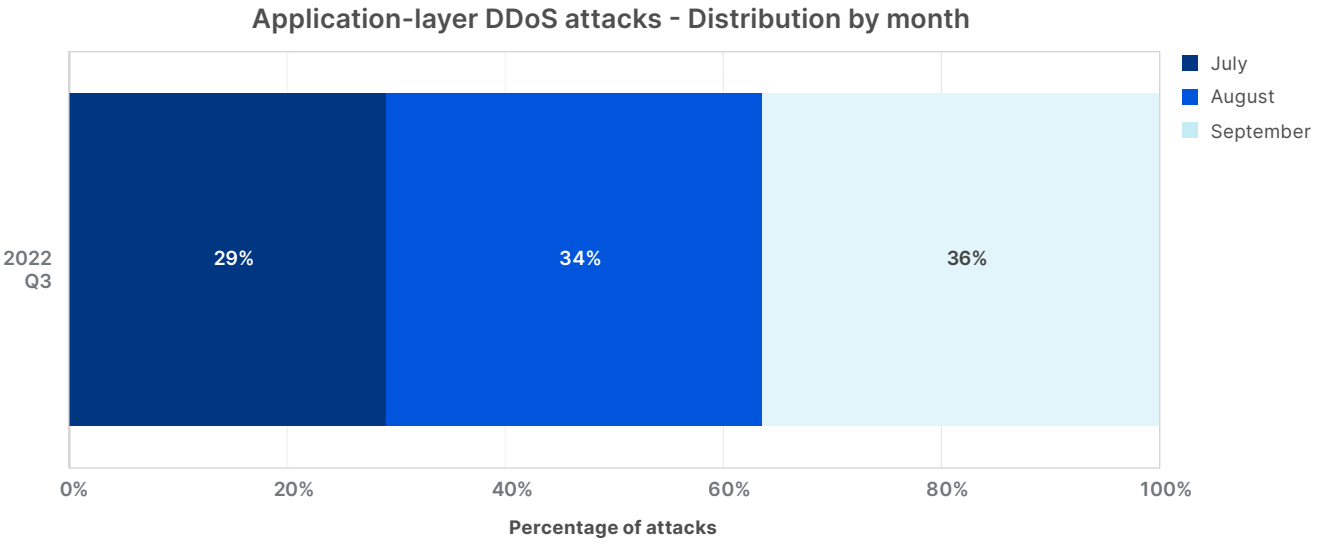


A diagram of an application-layer DDoS attack denying service to legitimate users

The graph below shows an approximately 10% decrease in attacks in each quarter since 2022 Q1. However, despite the downward trend, when comparing Q3 of 2022 to Q3 of 2021, HTTP DDoS attacks still increased by 111% year-over-year.



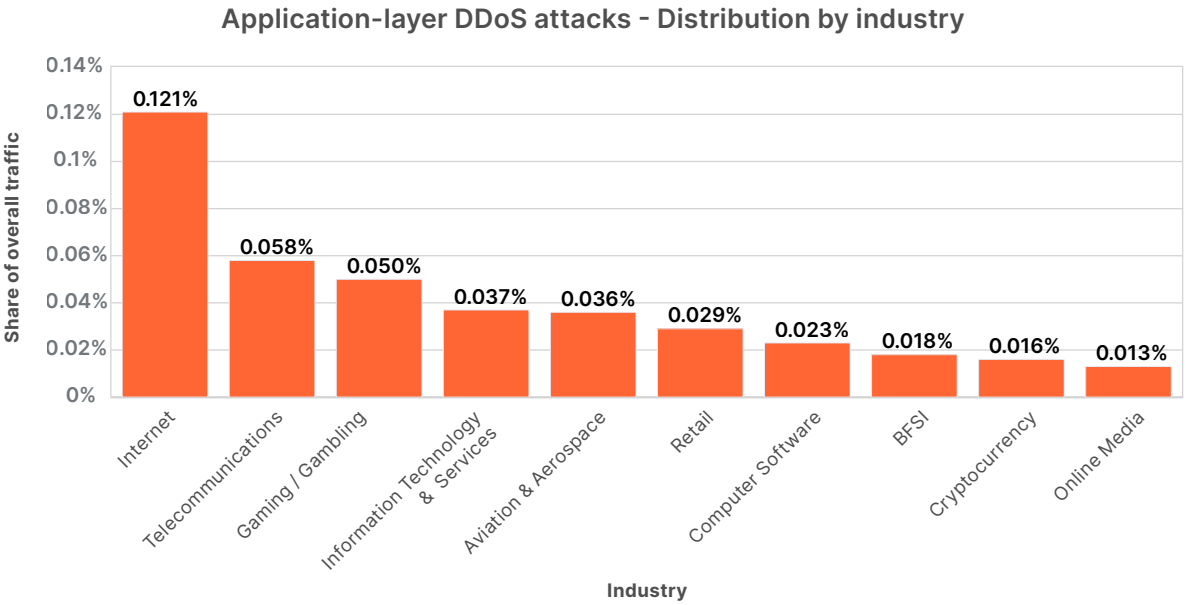
On a month-by-month basis, attacks in September and August were fairly evenly distributed; 36% and 35% respectively. In July, the amount of attacks slightly declined to 29%.



Application-layer DDoS attacks by industry

By analyzing the attacks based on customers' industry of operation, we can see that HTTP applications operated by Internet companies were the most targeted in the third quarter. Attacks on the Internet industry increased by 131% quarter-over-quarter and 300% year-over-year.

The second most attacked industry was the telecommunications industry, with an increase of 93% quarter-over-quarter and an astounding 2,317% increase year-over-year. In third place was the gaming and gambling industry, which saw a more conservative increase of 17% quarter-over-quarter and 36% increase year-over-year.

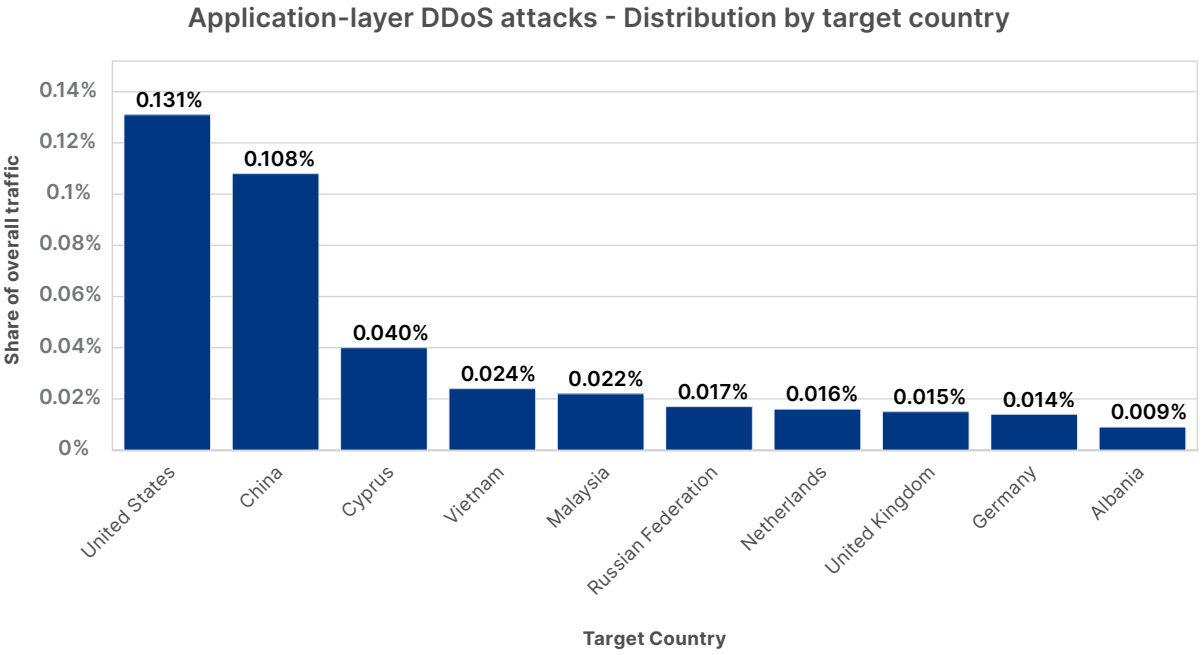


Application-layer DDoS attacks by target country

Categorizing attacks by our customers' billing address gives us an understanding of which countries are experiencing more attacks. HTTP applications operated by United States companies were the most targeted in the third quarter. Attacks targeting US-based websites saw an increase of 60% quarter-over-quarter and 105% increase year-over-year. Meanwhile, attacks targeting China increased by 332% quarter-over-quarter and increased by 800% year-over-year.

Looking at Ukraine, our data showed that attacks targeting Ukrainian websites increased by 67% quarter-over-quarter but decreased by 50% year-over-year. Furthermore, attacks targeting Russian websites increased by 31% quarter-over-quarter and sharply increased by 2,400% year-over-year.

In East Asia, attacks targeting Taiwanese companies increased by 200% quarter-over-quarter and increased by 60% year-over-year. Additionally, attacks targeting Japanese companies increased by 105% quarter-over-quarter.



Top countries targeted by HTTP DDoS attacks

When we zoom in on specific countries, the below trends may reveal interesting insights regarding the war in Ukraine and geopolitical events in East Asia:

- In Ukraine, we saw a notable change in the most attacked industries. In Q1 and Q2 of this year, Broadcasting, Online Media and Publishing companies were targeted most often — perhaps as part of an attempt to reduce civilians' access to information. However, this quarter, those industries dropped out of the top 10 list. Instead, the Marketing & Advertising industry took the lead (40%), followed by Education (20%), and Government Administration (8%).

- In Russia, attacks targeting the Banking, Financial Services and Insurance (BFSI) industry continue to persist most frequently (25%), though attacks on the BFSI sector still decreased by 44% quarter-over-quarter. The second most attacked industry was Events Services (20%), followed by Cryptocurrency (16%), Broadcast Media (13%), and Retail (11%). A significant portion of the attack traffic came from Germany-based IP addresses, and the rest were globally distributed.
- In Taiwan, the two most attacked industries were Online Media (50%) and Internet (23%). Attacks to those industries were globally distributed, indicating the usage of botnets.
- In Japan, the most attacked industry was Internet/Media & Internet (52%), Business Services (12%), and National Government (11%).

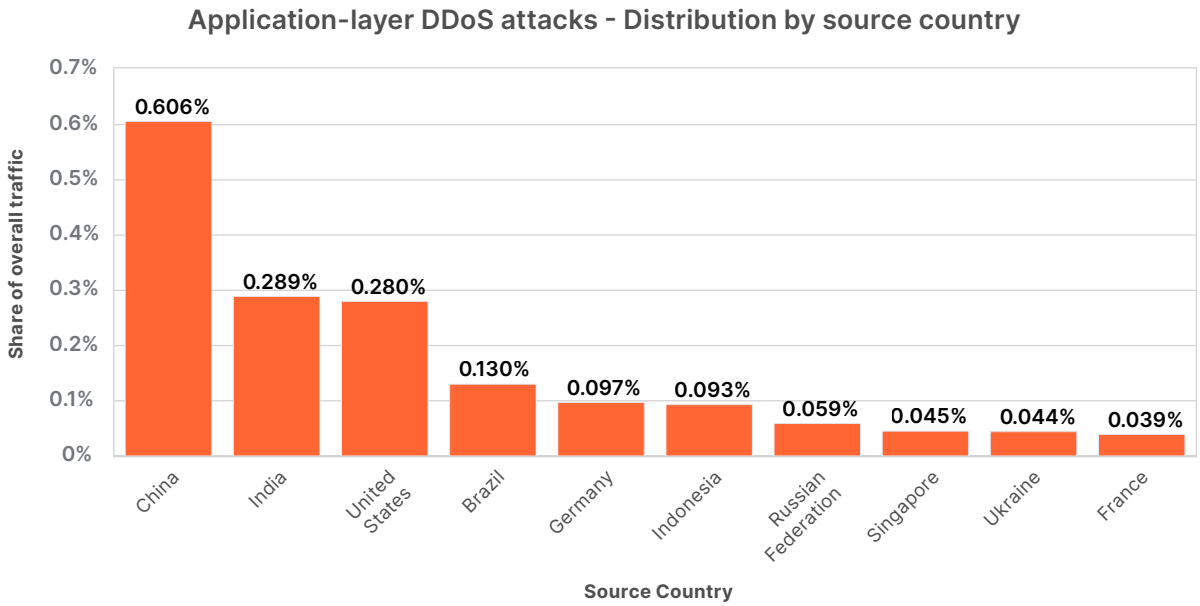
Application-layer DDoS attack traffic by source country

Before digging into source country metrics, it is important to note that an attack's country of origin is not necessarily indicative of where the attacker is located. DDoS attacks are often launched remotely, and attackers will go to great lengths to hide their actual location in an attempt to avoid being caught. If anything, attack sources indicate where botnet nodes are located. With that being said, by mapping an attacking IP address to a location, we can understand where attack traffic is coming from.

This quarter, China replaced the US as the main source of HTTP DDoS attack traffic. Attack traffic from China-registered IP addresses increased by 29% year-over-year and 19% quarter-over-quarter. Following China, India was the second-largest source of HTTP DDoS attack traffic — an increase of 61% year-over-year. After India, the main sources of attack traffic were the US and Brazil.

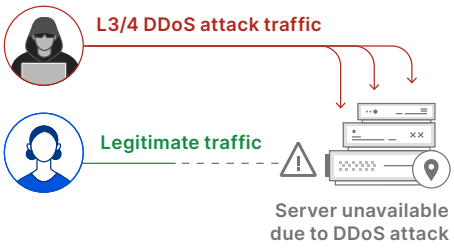
Looking at Ukraine, we can see that this quarter there was a drop in attack traffic originating from Ukrainian and Russian IP addresses — decreases of 29% and 11% quarter-over-quarter, respectively. However, year-over-year attack traffic from within those countries increased by 47% and 18%, respectively.

Attack traffic originating from Japanese IP addresses increased by 130% year-over-year.



Network-layer DDoS attacks

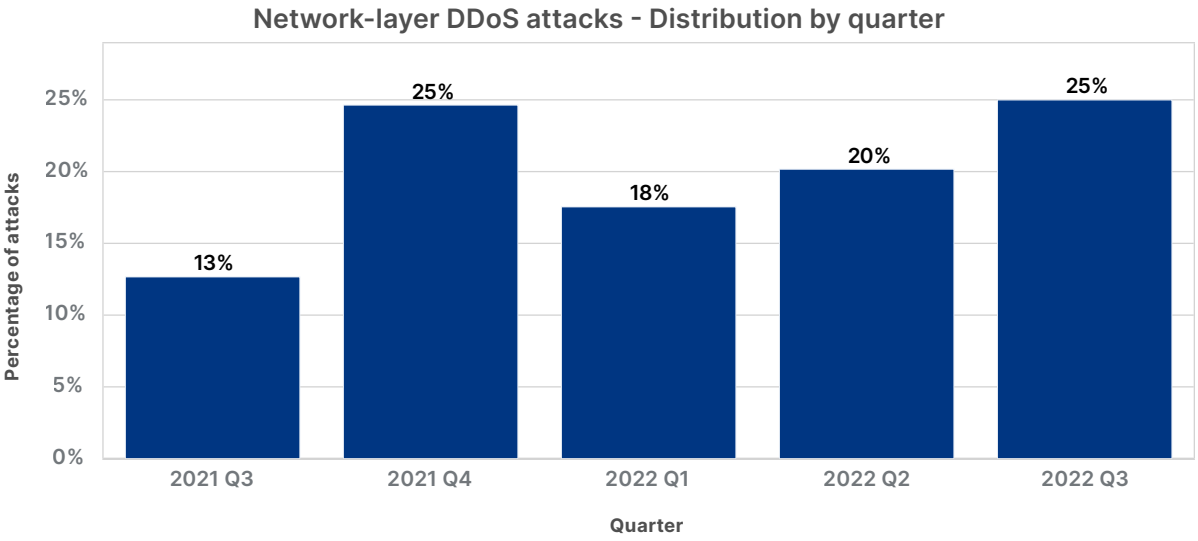
While application-layer attacks target the application (Layer 7 of the OSI model) running the service that end users access (HTTP/S in our case), network-layer attacks aim to overwhelm network infrastructure (such as in-line routers and servers) and the Internet link itself.



A diagram of an network-layer DDoS attack denying service to legitimate users

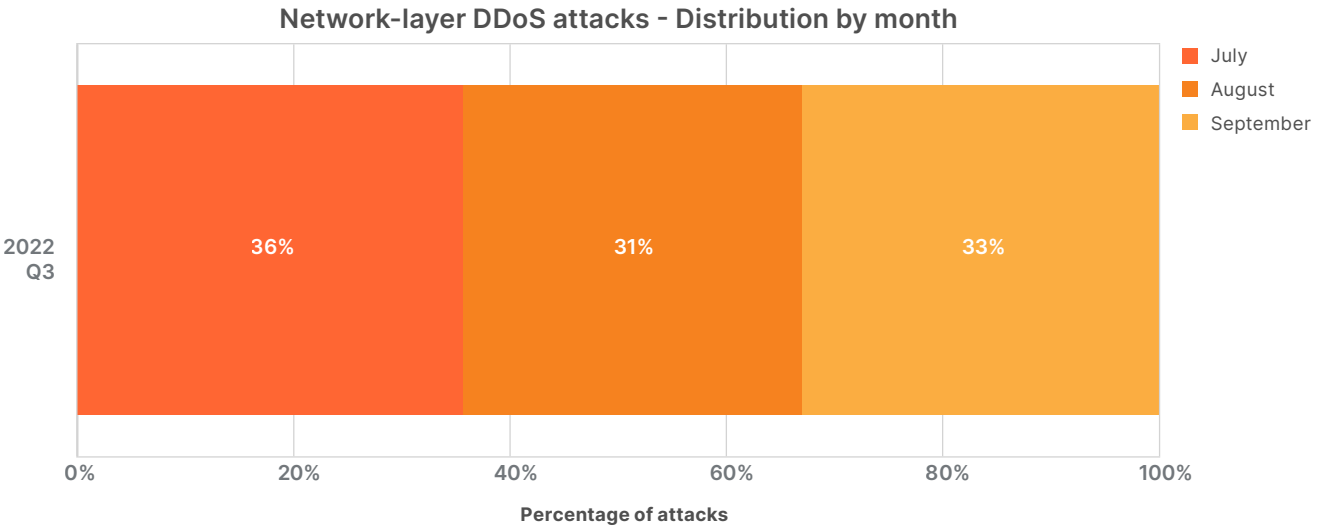
Network-layer DDoS attack trends

In the third quarter, we saw a large surge in L3/4 DDoS attacks — an increase of 97% year-over-year and a 24% quarter-over-quarter. The graph below shows a trend over the past three quarters of an increase in network-layer attacks.



Distribution of L3/4 DDoS attacks by quarter

This quarter attacks were evenly distributed throughout the three months, with a slightly larger share of attacks taking place in July.

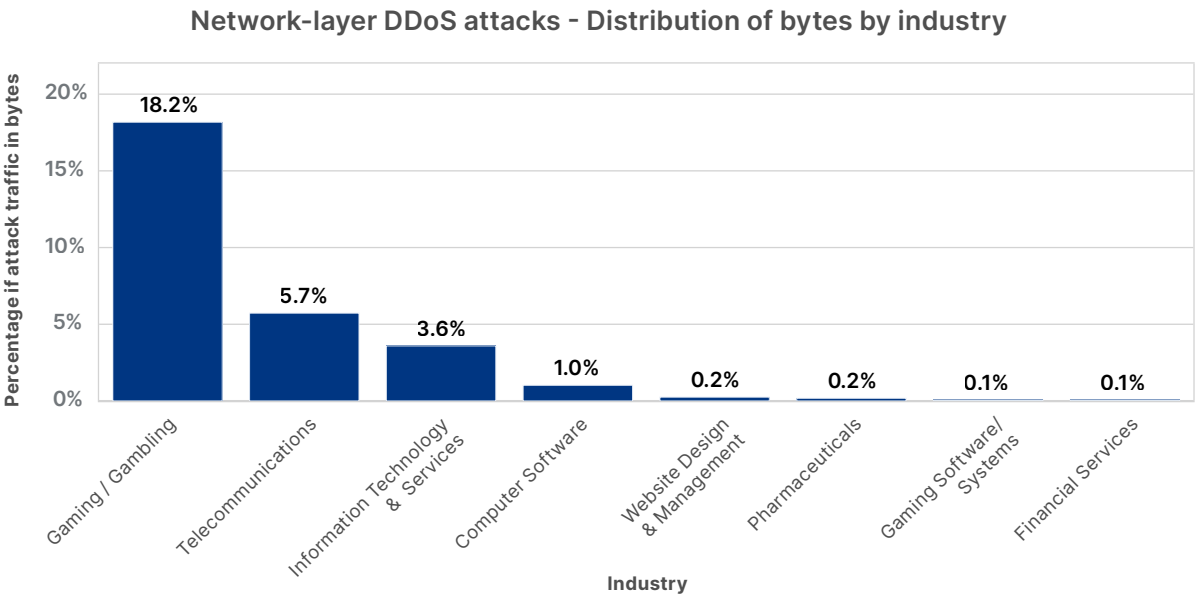


Network-layer DDoS attacks by Industry

The gaming and gambling industry was hit by the most L3/4 DDoS attacks in the third quarter. Almost one out of every five bytes Cloudflare ingested towards gaming and gambling networks were part of a DDoS attack. This represents a stark 381% increase quarter-over-quarter.

The second most targeted industry was telecommunications. In fact, almost 6% of bytes directed towards telecommunications networks were part of DDoS attacks. This represents a 58% drop from the previous quarter, where telecommunications was the top most attacked industry for network-layer DDoS attacks.

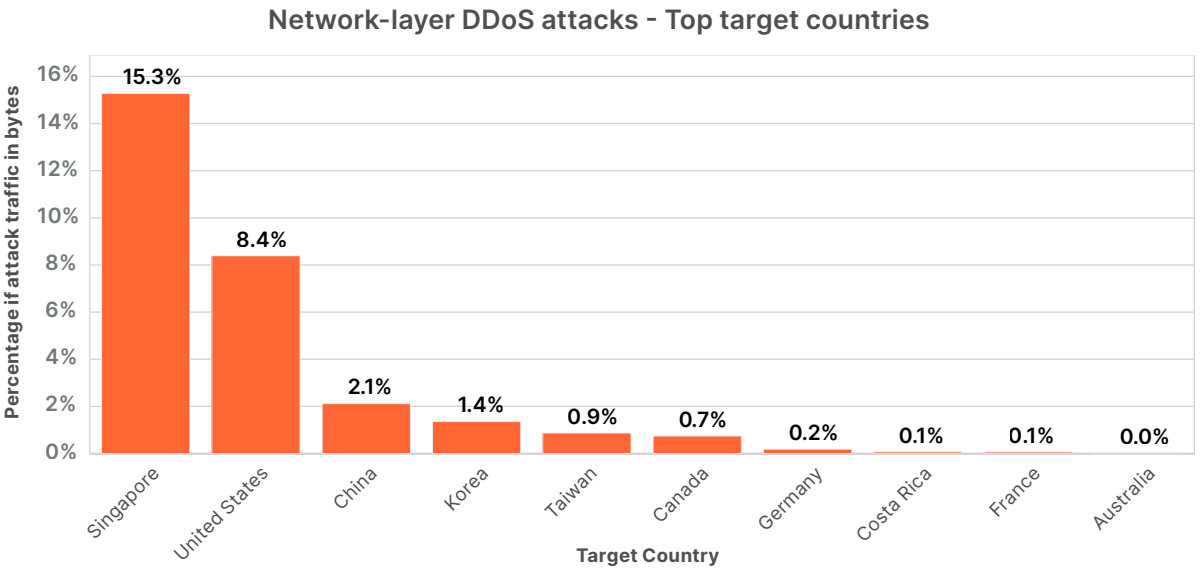
The third and fourth most attacked industries were information technology/services and software. Both saw significant growth in attacks — an 89% increase for information technology/services industry and a 150% increase for the software industry quarter-over-quarter.



Network-layer DDoS attacks by target country

Singapore-based companies saw the most L3/4 DDoS attacks, where over 15% of all bytes sent to their networks were associated with a DDoS attack. This represents a dramatic 1,175% increase quarter-over-quarter.

US-based companies came in second place, after a 45% decrease quarter-over-quarter in attack traffic targeting US networks. In third, China networks saw a 62% quarter-over-quarter increase. Attacks on Taiwan companies increased by 200% quarter-over-quarter.



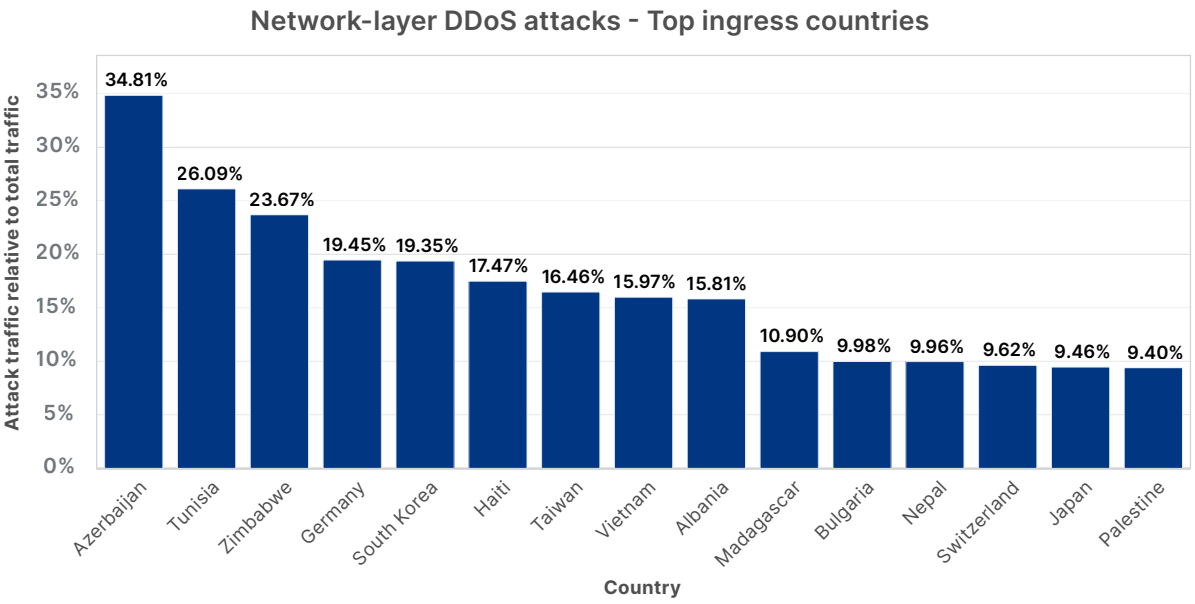
Network-layer DDoS attacks by ingress country

In the third quarter, Cloudflare data centers in Azerbaijan saw the largest percentage of attack traffic. More than a third of all packets ingested there were part of a L3/4 DDoS attack. This represents a 44% increase quarter-over-quarter and a huge 59-fold increase year-over-year.

Similarly, our data centers in Tunisia saw a dramatic increase in attack packets — 173x the amount in the previous year. Zimbabwe and Germany also saw significant increases in attacks.

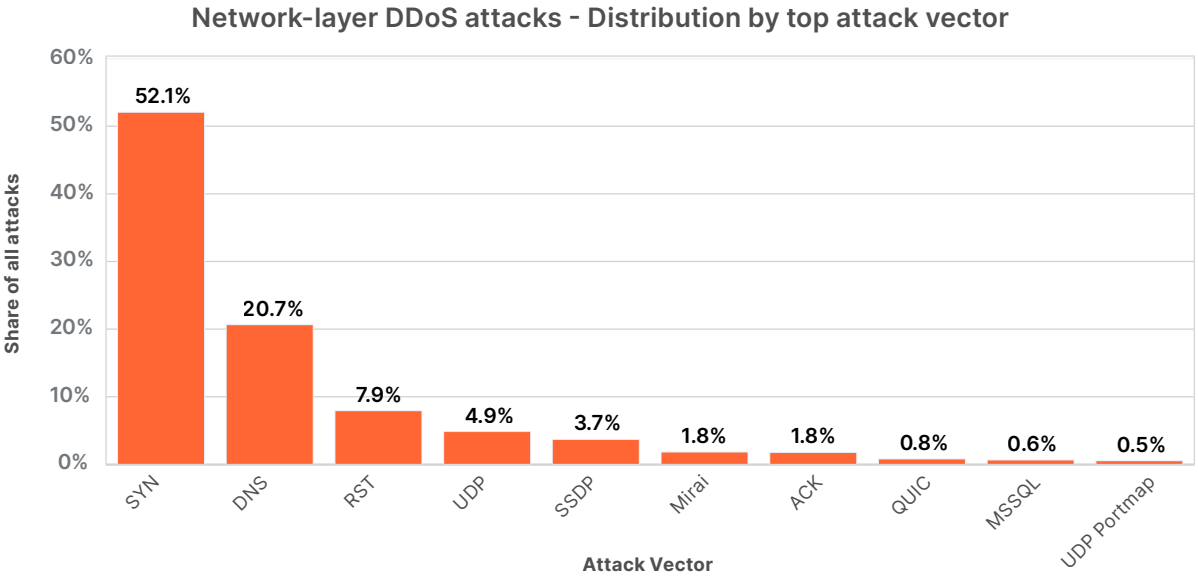
Zooming in on East Asia, we can see that our data centers in Taiwan saw an increase of attacks — 207% quarter-over-quarter and 1,989% year-over-year. We saw similar numbers in Japan, where attacks increased by 278% quarter-over-quarter and 1,921% year-over-year.

Looking at Ukraine, we saw a dip in the amount of attack packets we observed in our Ukraine-based and Russia-based data centers — 49% and 16% quarter-over-quarter, respectively.



Attack vectors & emerging threats

An attack vector is the method used to launch the attack or the method of attempting to achieve denial-of-service. With a combined share of 71%, SYN floods and DNS attacks remained the most popular DDoS attack vectors in the third quarter.



Top attack vectors

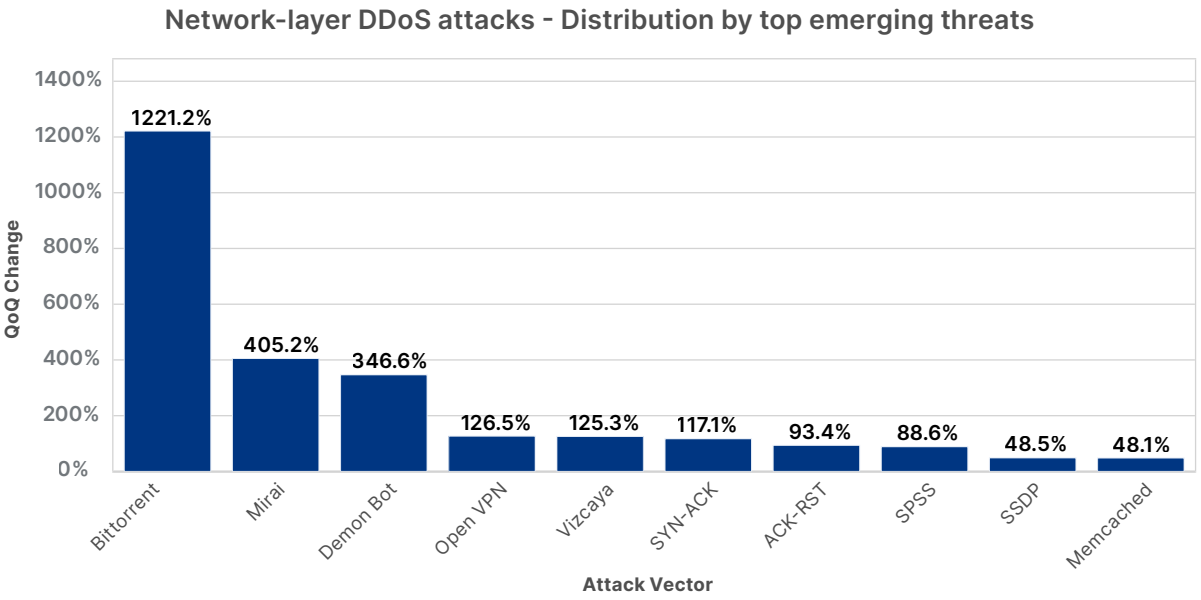
In the third quarter, we saw a resurgence of attacks abusing the CHARGEN protocol, attacks using the Ubiquity Discovery Protocol, and Memcached reflection attacks. While the growth in Memcached DDoS attacks also slightly grew (48%), this quarter, there was a more dramatic increase in attacks abusing the BitTorrent protocol (1,221%), as well as in attacks launched by the Mirai botnet and its variants.

BitTorrent DDoS attacks increased by 1,221% quarter-over-quarter

The BitTorrent protocol is a communication protocol used for peer-to-peer file sharing. To help BitTorrent clients find and download the files efficiently, BitTorrent clients may use BitTorrent Trackers or Distributed Hash Tables (DHT) to identify the peers seeding the desired file. This concept can be abused to launch DDoS attacks. A malicious actor can spoof the victim's IP address as a seeder IP address within Trackers and DHT systems. Then, clients would request the files from those IPs. Given a sufficient number of clients requesting the file, it can flood the victim with more traffic than it can handle.

Mirai DDoS attacks increased by 405% quarter-over-quarter

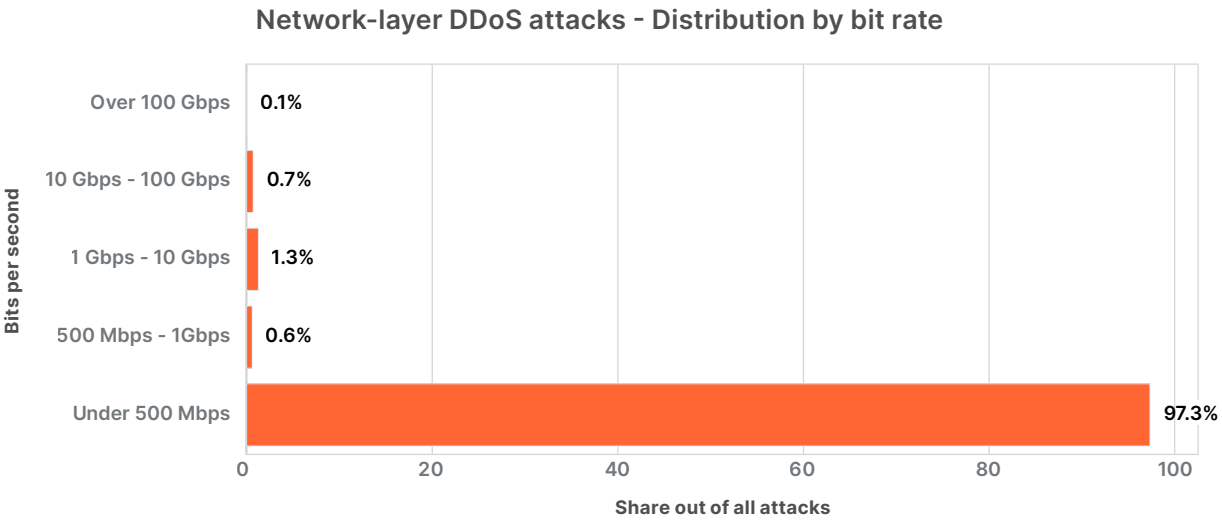
Mirai is malware that infects smart devices running on ARC processors — turning them into a network of bots, or "zombies", that can be used to launch DDoS attacks. This processor runs a stripped-down version of the Linux operating system. If the default login credentials are not changed, Mirai is able to login to the device, infect it, and take over. The botnet operator can instruct the botnet to launch a flood of UDP packets at the victim's IP address to bombard them.



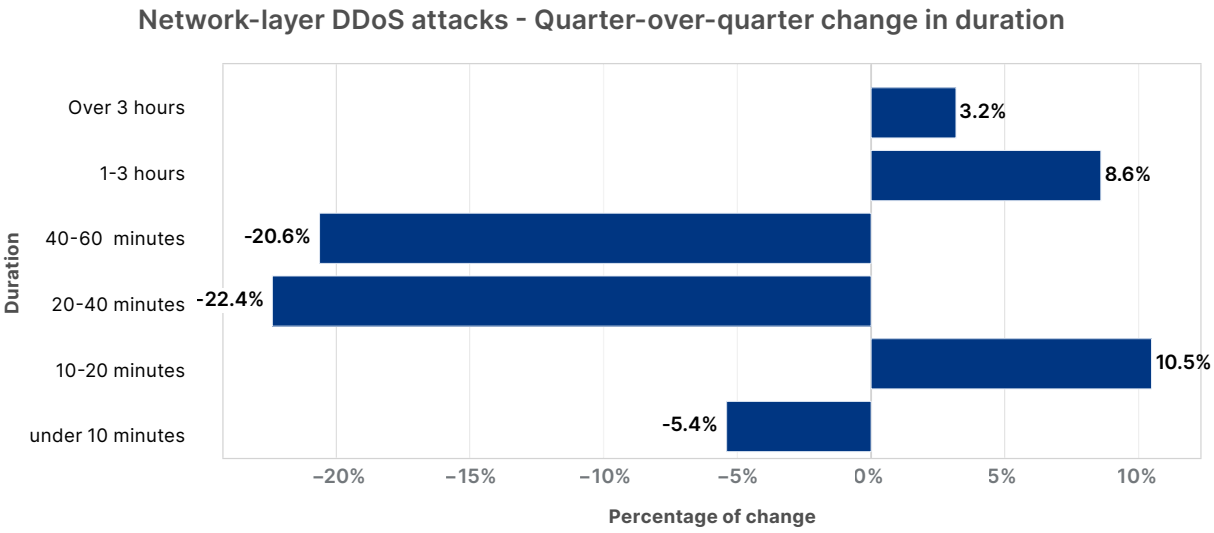
Network-layer DDoS attacks by attack rates and duration

While Terabit-strong attacks are becoming more frequent, they are still the outliers. The majority of attacks are tiny (in terms of Cloudflare scale). Over 95% of attacks peaked below 50,000 packets per second (pps) and over 97% below 500 Megabits per second (Mbps). We call this “cyber vandalism.”

Cyber vandalism is the act of causing deliberate damage to Internet properties. Today, the source codes for various botnets are available online, and there are a number of free tools that can be used to launch a flood of packets. By directing those tools at Internet properties, any person with scripting knowledge can use those tools to launch attacks against Internet properties. We consider cyber vandalism different from organized crime, Advanced Persistent Threat (APT) actors, or state-level actors, as those types of attacks are usually larger and more sophisticated.



Similarly, most of the attacks are very short and end within 20 minutes (94%). This quarter we did see an increase of 9% in attacks of 1-3 hours, and a 3% increase in attacks over 3 hours — but those are still the outliers.



Even with the largest attacks — such as the 2.5 Tbps attack on Wynncraft we mitigated earlier this quarter and the 26M request per second attack we mitigated back in the summer — the peak of the attacks were short-lived. The entire 2.5 Tbps attack lasted about 2 minutes, and the peak of the 26M rps attack only lasted 15 seconds.

This emphasizes the need for automated, always-on solutions, because security teams simply can't respond quick enough to attacks this short. By the time the engineer looks at the PagerDuty notification on their phone, the attack will have subsided.

Conclusion

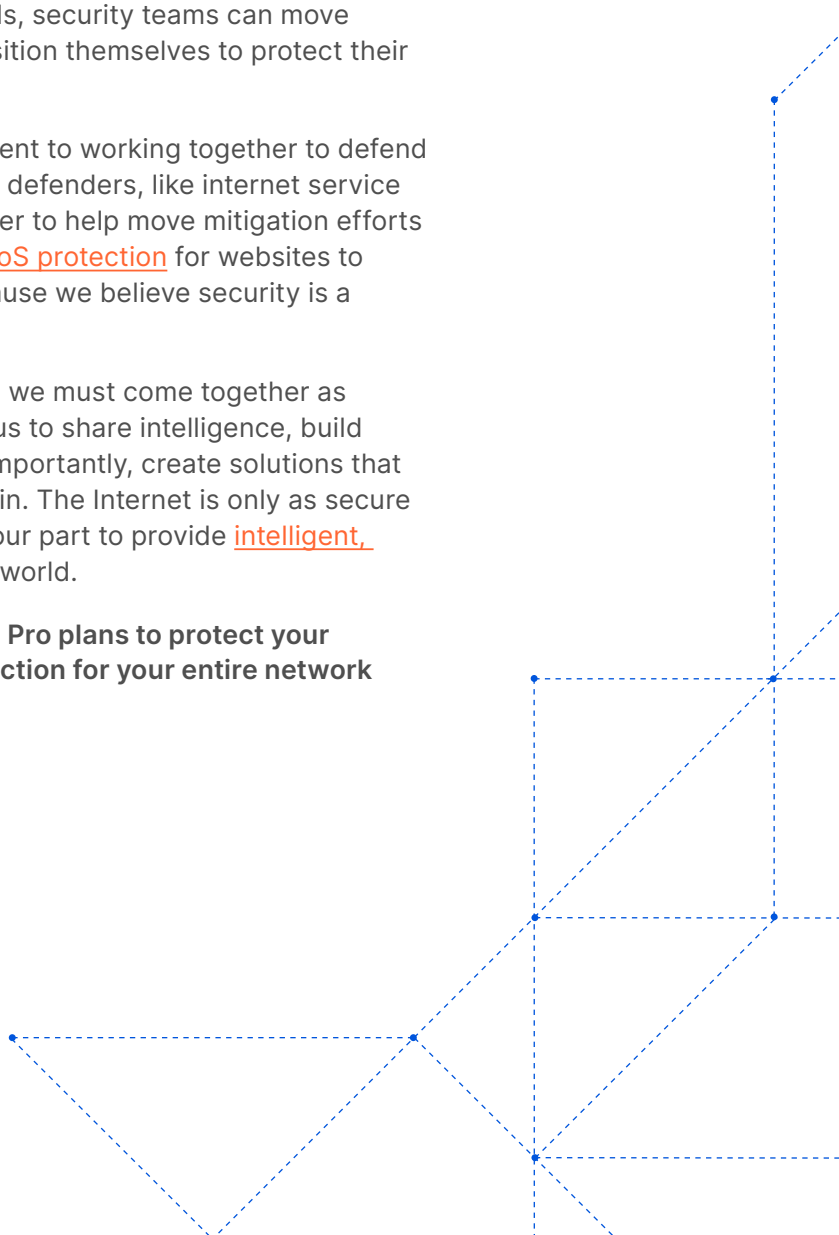
A multitude of factors contribute to the continued presence of DDoS attacks around the world. DDoS attacks continue to become cheaper, easier, and more accessible for attackers. To make matters worse, billions of IoT devices deployed around the world lack effective security, making them an easy target for exploitation. As we saw with the Mirai botnet, open-sourced DDoS code can live on, mutate, and gain widespread adoption long after its creators have been caught and punished.

To defend against DDoS attacks, humans must fight bots with bots. Botnets require infected devices to carry out their mission, so the more devices we protect from day one, the fewer botnets will emerge. Default settings of IoT devices are not secure, and there is a clear need for more effective detection and remediation of infected devices. The longer botnets are allowed to operate freely, the bigger and stronger they grow, and the harder they become to stop. With the right tools, security teams can move from a reactive state to a proactive one, and better position themselves to protect their organizations.

Mitigating DDoS attacks requires a collective commitment to working together to defend the Internet against threats. Cloudflare helps upstream defenders, like internet service providers (ISPs), with our free botnet threat feed in order to help move mitigation efforts closer to the source. We also offer free, unmetered DDoS protection for websites to millions of Internet users. We offer these services because we believe security is a fundamental piece of a better Internet.

In order to improve the current DDoS threat landscape, we must come together as defenders of the free and open Internet. It will require us to share intelligence, build tools that interoperate with one another — and, most importantly, create solutions that are easy to implement, easy to use, and easy to maintain. The Internet is only as secure as its weakest link, and Cloudflare will continue doing our part to provide intelligent, always-on DDoS defense to our customers around the world.

Not using Cloudflare yet? Start now with our Free and Pro plans to protect your website, or contact us for comprehensive DDoS protection for your entire network using Magic Transit.



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3874.2022OCT21