CLOUDFLARE

Cloudflare DDoS Trends Report

Content

Q4 2023

Executive Summary

Welcome to the sixteenth edition of the Cloudflare DDoS Threat Report. DDoS attacks, or distributed denial-of-service attacks, are a type of cyber attack that aims to disrupt websites (and other types of Internet properties) to make them unavailable for legitimate users by overwhelming them with excessive traffic. Think of it as causing a traffic jam on a critical road, preventing people from reaching their destination.

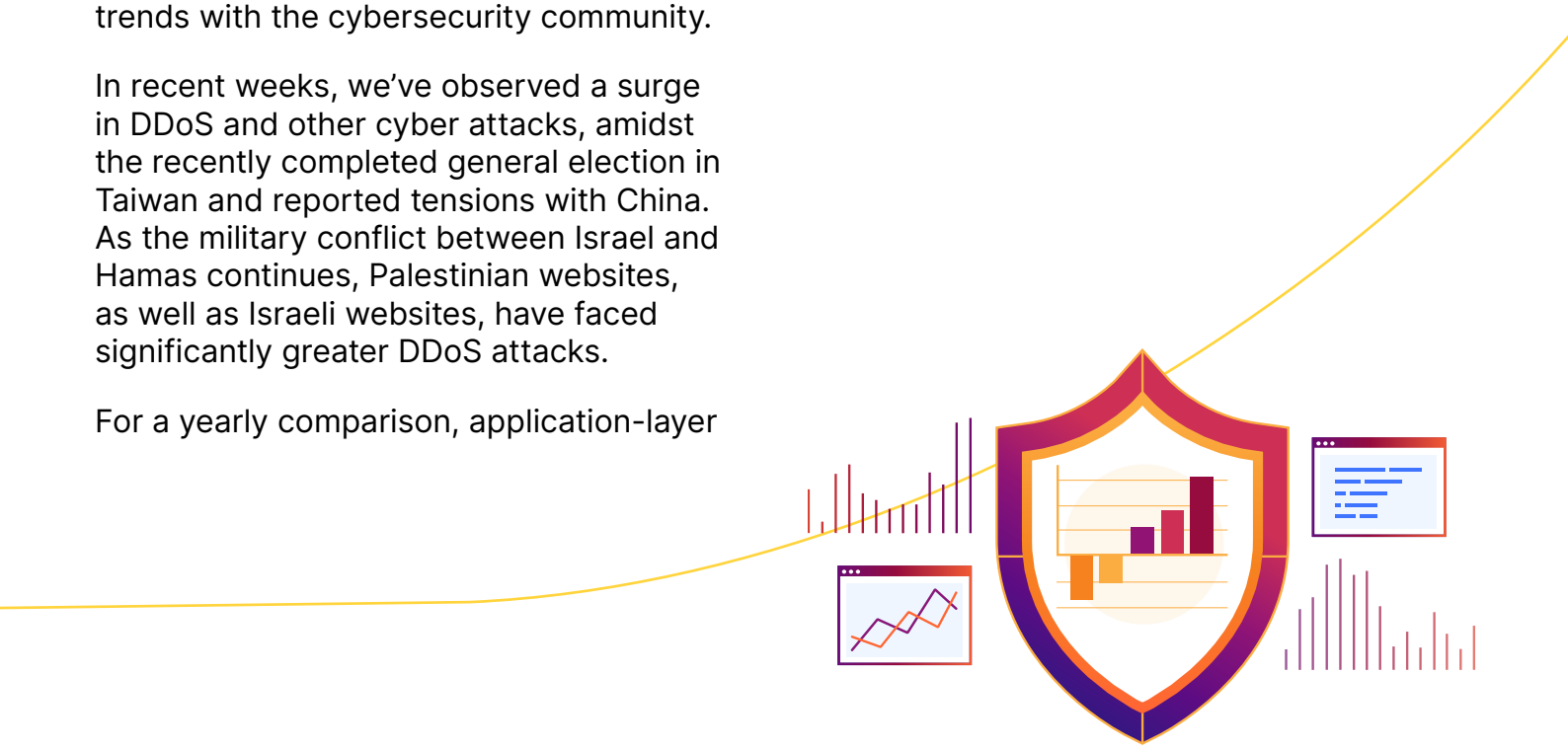
Our network is one of the largest in the world, spanning more than 310 cities in over 120 countries. We handle a massive amount of internet traffic, serving over 70 million web requests per second at its peak and processing 2.6 billion DNS queries daily. On average, we thwart 170 billion cyber threats each day. This vast data volume provides us with a unique perspective on the DDoS threat landscape, enabling us to share valuable insights and trends with the cybersecurity community.

In recent weeks, we've observed a surge in DDoS and other cyber attacks, amidst the recently completed general election in Taiwan and reported tensions with China. As the military conflict between Israel and Hamas continues, Palestinian websites, as well as Israeli websites, have faced significantly greater DDoS attacks.

For a yearly comparison, application-layer DDoS attacks drop by 20% year on year in 2023 compared to 2022. Ironically, 2023 has also seen the largest application-layer DDoS attack campaigns crossing 100M requests per second in multiple instances, including the HTTP/2 Rapid Reset attack campaign earlier this year. At the network-layer, we saw a completely different trend: a 85% increase of network-layer DDoS attacks in 2023 compared to 2022.

Notably, environmental services organizations experienced the highest volume of HTTP DDoS attack traffic, which coincided with the 28th United Nations Climate Change Conference (COP 28).

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



Report Highlights

DDoS Trends for the year 2023

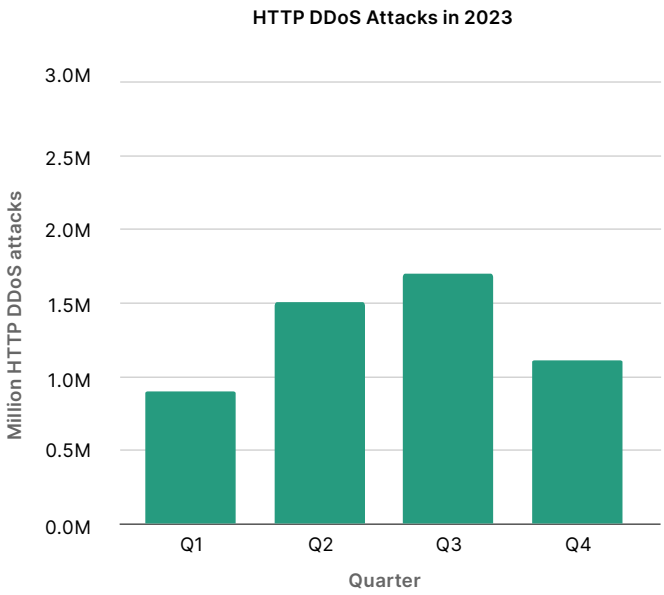
After the hyper-volumetric campaign subsided, we saw an unexpected drop in HTTP DDoS attacks by 20% compared to 2022. Overall in 2023, our automated defenses mitigated over 5.2 million HTTP DDoS attacks consisting of over 26 trillion requests. Despite the drop in number of attacks, the average number of attacks stopped is very large: 594 HTTP DDoS attacks stopped and 3 billion requests mitigated every hour of 2023.

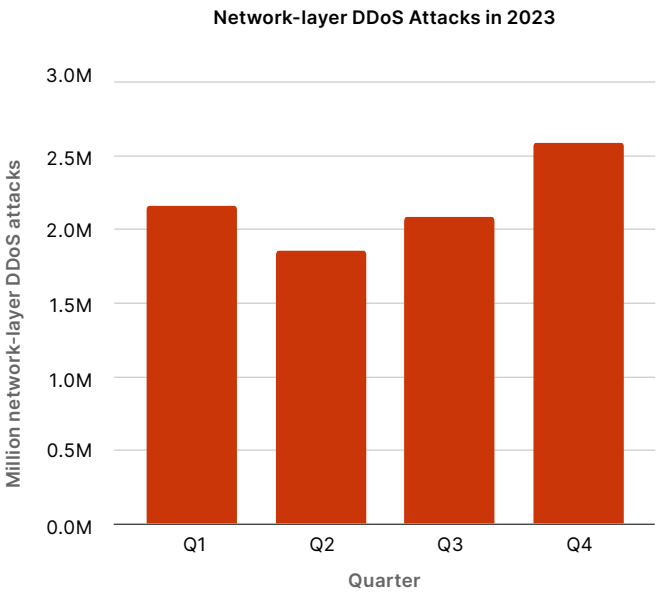
On the network-layer, we saw a completely different trend. Our automated defenses mitigated 8.7 million network-layer DDoS attacks in 2023. This represents an 85% increase compared to 2022. On average, our systems mitigated 996 network-layer DDoS attacks and 27 terabytes every hour.

2023 - DDoS Attacks in Numbers

↓ **HTTP DDoS attacks**
5.2 million attacks
mitigated in 2023
-20% YoY

↑ **Network-layer DDoS attacks**
8.7 million attacks
mitigated in 2023
+85% YoY





Specific conflict zones and DDoS attacks: Taiwan general election and Israel Hamas conflict

The surge in attacks targeting specific regions (Taiwan, Israel, and Palestinian territories) underscores the use of DDoS as a tool in cyber warfare, leveraging cyber capabilities to exert political pressure or disrupt critical digital infrastructure.

Taiwan general elections

We saw a 3,370% year on year increase in HTTP DDoS attacks targeting websites in Taiwan. The vast majority (82%) originated from China, which is correlated with the heated political rhetoric in China and Taiwan right now. Surprisingly, adult entertainment websites were targeted more than common industries entrenched in daily life such as financial services, healthcare, and transportation industries.

Israel-Hamas war

DDoS attacks are an accepted tool of war and disruption. We witnessed an increase in DDoS attack activity in the Ukraine-Russia war, and now we're also witnessing it in the Israel-Hamas war. We first reported the cyber activity in our Cyber attacks in the Israel-Hamas war blog post, and we continue to monitor the activity till date.

The Palestinian territories were the second most attacked region in the world by HTTP and network layer DDoS attacks in Q4. DDoS attacks accounted for over 68% of all their layer 3 and layer 4 traffic to Palestinian networks and more than 10% of all HTTP requests to Palestinian websites. 9 out 10 of these HTTP DDoS attacks targeted Palestinian banking websites.

Israeli websites also saw heavy DDoS traffic, although they saw a more modest 27% increase in quarter over quarter HTTP DDoS traffic. The newspaper & media and computer software industries received almost 65% of all HTTP DDoS attacks on Israeli websites.

Our data suggests a concerted effort to hurt industries entrenched in daily life on both sides.

Growing trend of global political events triggering cyber attacks

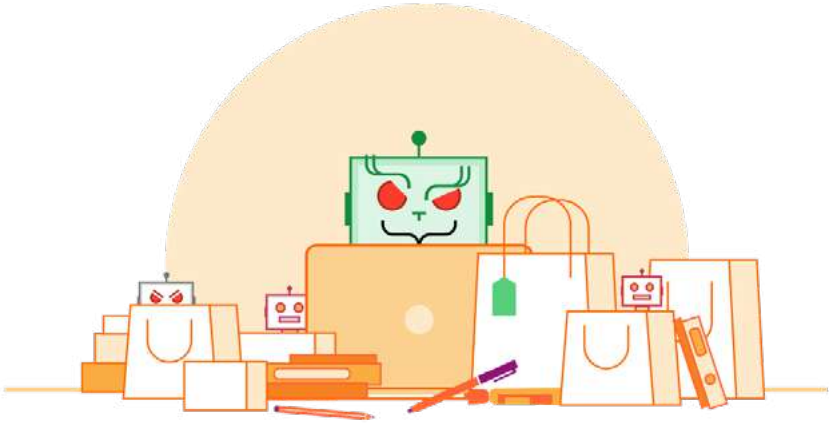
We are seeing a growing trend where global events can become trigger points for cyberattacks. The 28th United Nations Climate Change Conference (popularly known as COP 28) concluded on Dec 13, 2023. We saw a staggering (more than 61,000%) increase in HTTP DDoS attacks on environmental services organizations between October and Dec of 2023 compared to the same period in 2022. The pattern wasn't isolated to this event alone.

Looking back at historical data, particularly during COP 26 and COP 27, as well as other UN environment-related resolutions or announcements, a similar pattern emerges. Each of these events was accompanied by a corresponding increase in cyber attacks aimed at Environmental Services websites.

Q4 holiday season: The DDoS grinch

We saw increased HTTP DDoS activity targeting retail, shipment and public relations websites between Black Friday, Christmas and the new years holidays. At the application-layer, the packaging and freight delivery industry was the second most targeted (after the environmental services industry) relative to each industry's overall HTTP traffic. This industry underpins the success of the Black Friday and the winter holiday shopping experience. Purchased gifts and goods must get to their destination accurately and on time. Attackers may have tried to interfere with that. Application-layer DDoS attacks on retail companies also increased by 16% compared to the previous year, 2022.

On the network layer, the public relations (PR) and communications industry was the most targeted industry — 36% of its traffic was malicious. Disrupting this industry's operations can have immediate and widespread reputational impacts. The months of October to December and the end of year often see increased PR and communication activities due to holidays, end-of-year summaries, and preparations for the new year. In short, it is a critical operations period — one that attackers may want to disrupt.

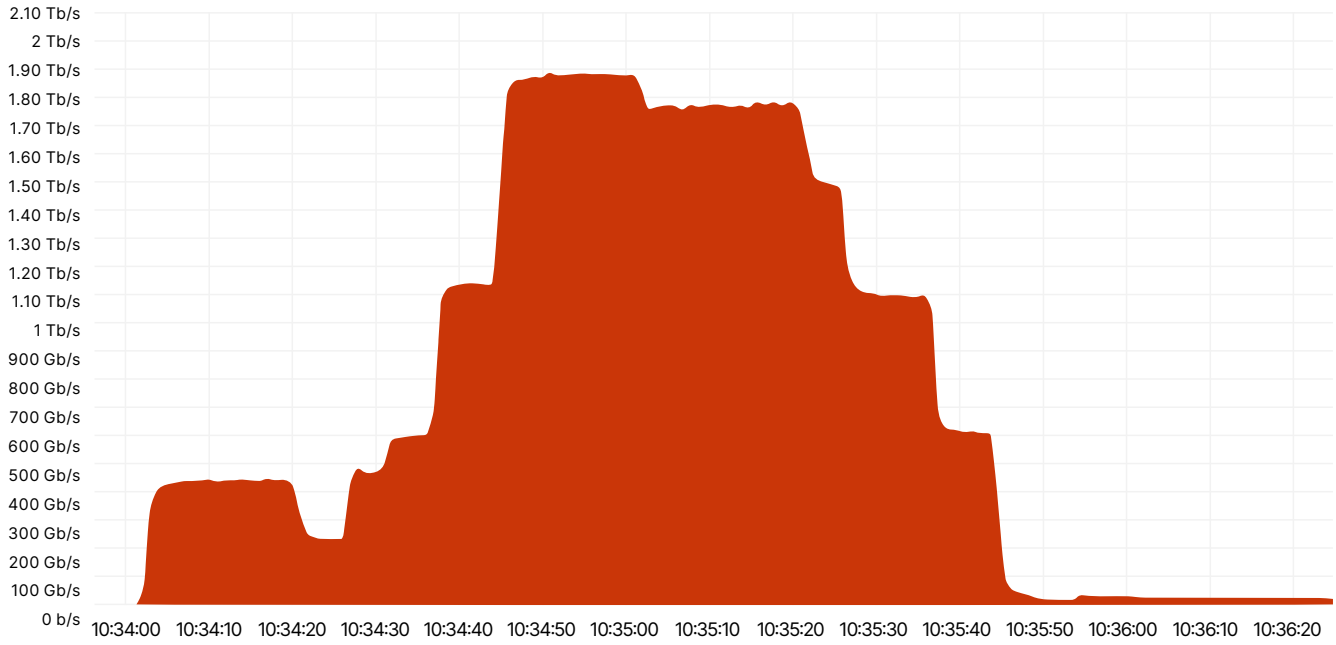


Emerging attack vectors at the network layer

Let's examine one specific attack to explore the changing landscape at network layer DDoS.

One of the large attacks between October and December 2023 was a Mirai-botnet attack that targeted a known European Cloud Provider for less than ten minutes and originated from over 18,000 unique IP addresses (assumed to be spoofed). It was automatically detected and mitigated by Cloudflare's defenses.

Major Mirai-botnet attack on European cloud provider

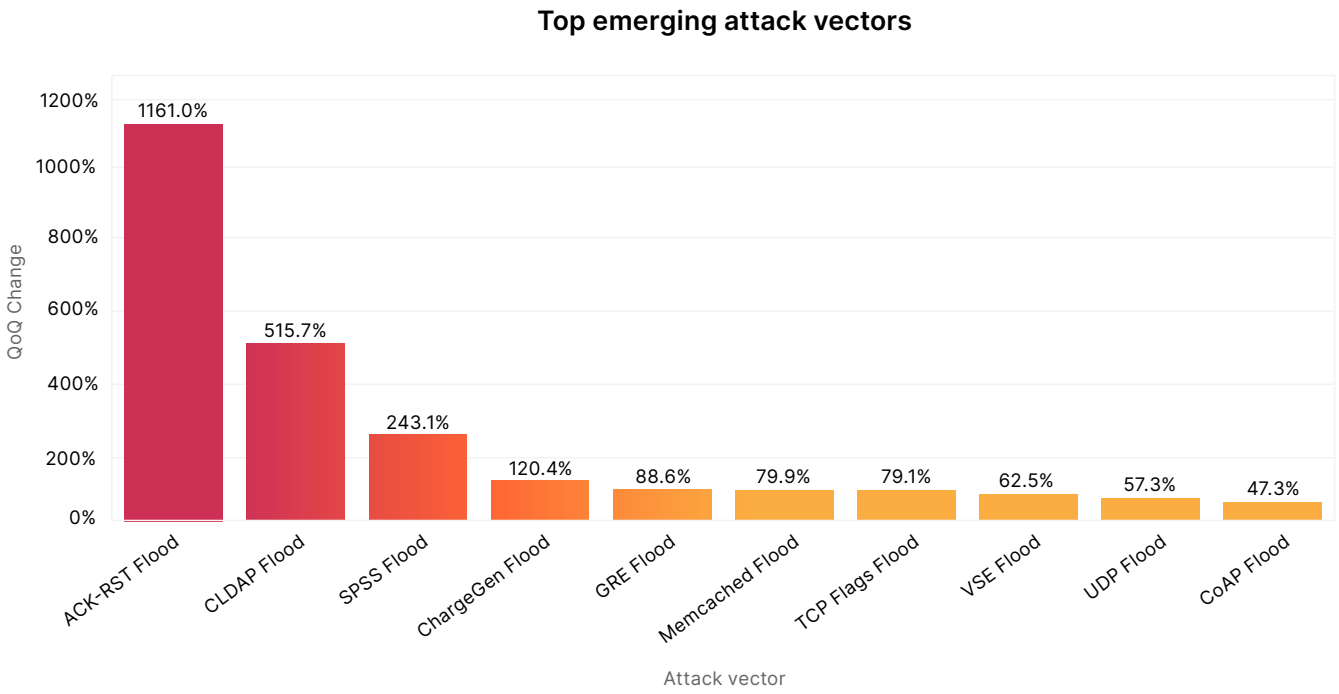


This attack was unique in terms of the high bits per second rate, multi-vector attack nature and yet lasted for only a short period. It peaked at 1.9 terabits per second and combined multiple attack methods including UDP fragments flood, UDP/Echo flood, SYN Flood, ACK Flood, and TCP malformed flags. Such large bits per second rate attacks are rare. Even more sophisticated is for attacks to combine multiple methods.

The packet per second rate at 160 million packets per second was not the largest we've ever seen, which was 754 million packets per second back in 2020.

Beyond this attack with its unique characteristics, organizations cannot afford to use manual scrubbing centers for their DDoS defenses. They need in-line automated defense systems.

Amongst the emerging threats we track, we recorded a 1,161% increase in ACK-RST Floods as well as a 515% increase in CLDAP floods, and a 243% increase in SPSS floods, in each case as compared to last quarter. Let's walk through some of these attacks and how they're meant to cause disruption.



ACK-RST floods

An ACK-RST Flood exploits the Transmission Control Protocol (TCP) by sending numerous ACK and RST packets to the victim. This overwhelms the victim's ability to process and respond to these packets, leading to service disruption. The attack is effective because each ACK or RST packet prompts a response from the victim's system, consuming its resources. ACK-RST Floods are often difficult to filter since they mimic legitimate traffic, making detection and mitigation challenging.

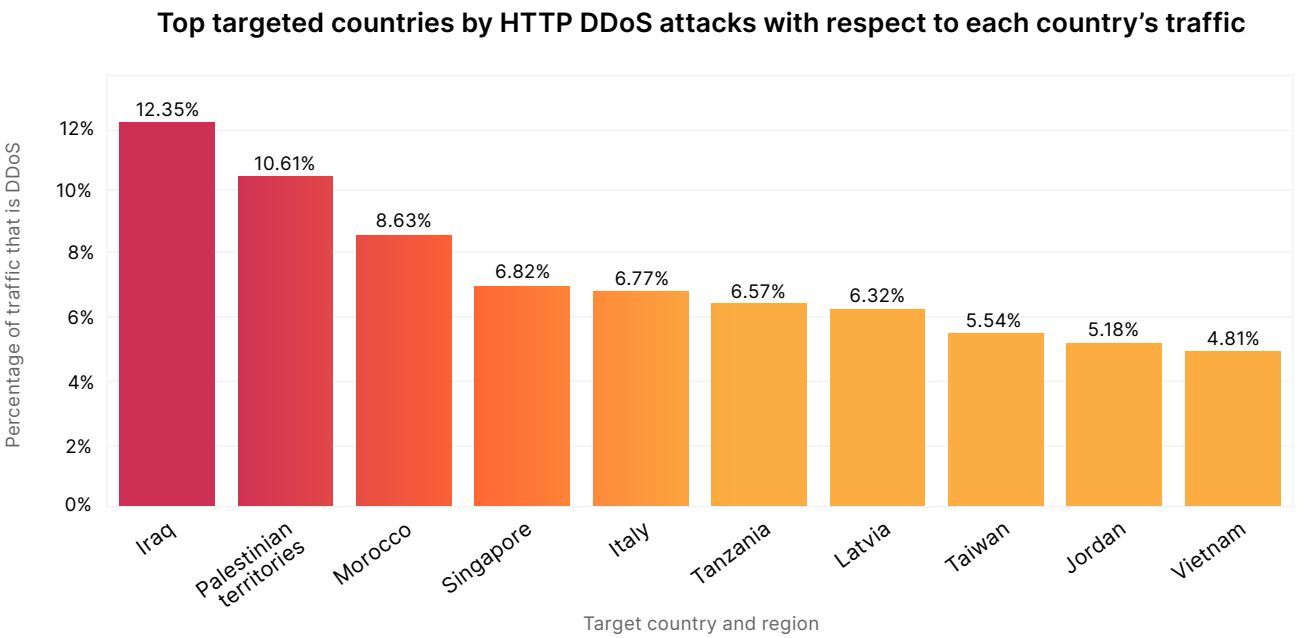
CLDAP floods

CLDAP (Connectionless Lightweight Directory Access Protocol) is a variant of LDAP (Lightweight Directory Access Protocol). It's used for querying and modifying directory services running over IP networks. CLDAP is connectionless, using UDP instead of TCP, making it faster but less reliable. Because it uses UDP, there's no handshake requirement which allows attackers to spoof the IP address thus allowing attackers to exploit it as a reflection vector. In these attacks, small queries are sent with a spoofed source IP address (the victim's IP), causing servers to send large responses to the victim, overwhelming it. Mitigation involves filtering and monitoring unusual CLDAP traffic.

SPSS floods

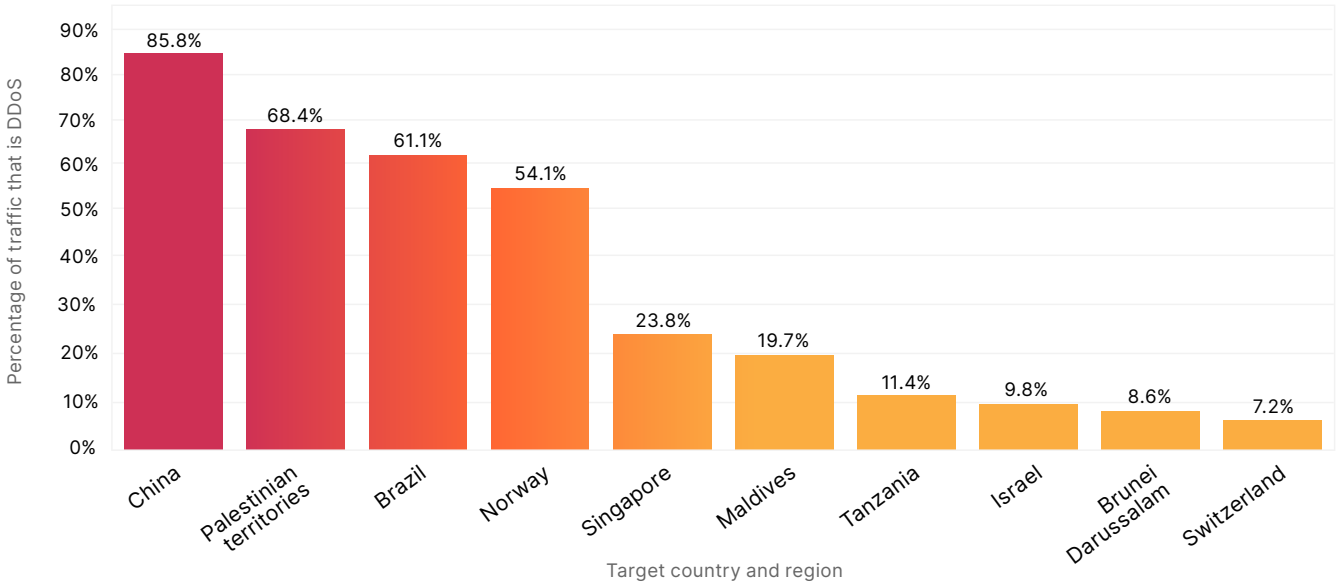
Floods abusing the SPSS (Source Port Service Sweep) protocol is a network attack method that involves sending packets from numerous random or spoofed source ports to various destination ports on a targeted system or network. The aim of this attack is two-fold: first, to overwhelm the victim's processing capabilities, causing service disruptions or network outages, and second, it can be used to scan for open ports and identify vulnerable services. The flood is achieved by sending a large volume of packets, which can saturate the victim's network resources and exhaust the capacities of its firewalls and intrusion detection systems. To mitigate such attacks, it's essential to leverage in-line automated detection capabilities.

Top attacked regions



Iraq, Palestinian territories, and Morocco take the lead as the most attacked regions with respect to their total inbound traffic. What's interesting is that Singapore comes up as fourth. Not only did Singapore face the largest amount of HTTP DDoS attack traffic (4% of all global DDoS traffic), but that malicious traffic also made up a significant amount of the total Singapore-bound HTTP traffic. By contrast, the US was second most attacked by volume of DDoS traffic (3.8% of all global DDoS traffic), but came in the fiftieth place when normalised by the total US-bound HTTP traffic.

Top targeted countries by Network-layer DDoS attacks with respect to each country's traffic



The network-layer trends by region are even more stark than at the application-layer.

China continues to be the most targeted country at the network layer in 2023. Even more dramatic than the HTTP DDoS trends for Singapore, China is both the number one most attacked country by network-layer DDoS attack traffic, and also with respect to all China-bound traffic. Almost 86% of all China-bound traffic was mitigated by Cloudflare as network-layer DDoS attacks. For three other regions, the Palestinian territories, Brazil, and Norway, more than 1 out of every 2 bytes to that region carried a DDoS attack.

Recommendations and takeaways

Best practices	Optimize your Cloudflare usage
Update or make a Denial of Service Response Plan.	Ensure your security vendor provides a 24/7 emergency hotline. Cloudflare Under Attack hotline will provide security expertise, process and technology to deal with attacks in real-time. Test your security vendors' incident response process and service level agreements (SLAs) before a real DDoS attack. Identify and train personnel on your documented DDoS response plan. Ensure they read through the Cloudflare DDoS learning path to optimize Cloudflare controls.
Deploy threat intelligence and in-line, automated DDoS mitigation solutions. Manual scrubbing centers do not scale with modern high-volume, short burst attacks.	Use multiple detection techniques to optimize your security posture in the face of the ever evolving threat landscape: 1. Dynamic stateless fingerprinting 2. Machine learning-based classification 3. Anomalous traffic detection 4. Traffic profiling and stateful mitigation 5. Threat intelligence on current DDoS activity and trends
Update your network, DNS and application infrastructure to be more resilient for your traffic profile.	Ensure capacity in your DDoS mitigation solution is large enough to handle twice the largest attacks on record and twice the max rates of your legitimate traffic. Ensure your security vendor can mitigate the latest network and application layer protocol vulnerabilities. Offload DNS traffic to compliant and secured cloud platforms with traffic routed through edge networks closest to the user.
Improve network and application performance to avoid bottlenecks.	Leverage a digital waiting room to ensure real users and visitors are gracefully informed of the waiting period without overwhelming application servers. Optimize caching, manage loads better with a content delivery network (CDN) and cloud based loading balancing solutions.
Use a positive security model: Ensure traffic that you want, gets in reliably.	Keep business critical protocols, IPs, ASNs, ports and user-agents open to clean traffic. Use schema validation and an API gateway for API traffic.
Leverage artificial intelligence to stay ahead of emerging threats.	Bot scores that can be used within firewall and rate-limiting rules. Automatically discover your public facing APIs and protect them from DDoS attacks.

At Cloudflare, we want to make it even easier — and free — for organizations of all sizes to protect themselves against even the largest and most complex DDoS attacks. We have been providing free unmetered and unlimited DDoS protection to all of our customers since 2017 — when we pioneered the concept.

Learn more about defending against the latest DDoS threats with Cloudflare.

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

REV:BDES-5497.2024FEB08