DDoS threat report for 2023 Q2

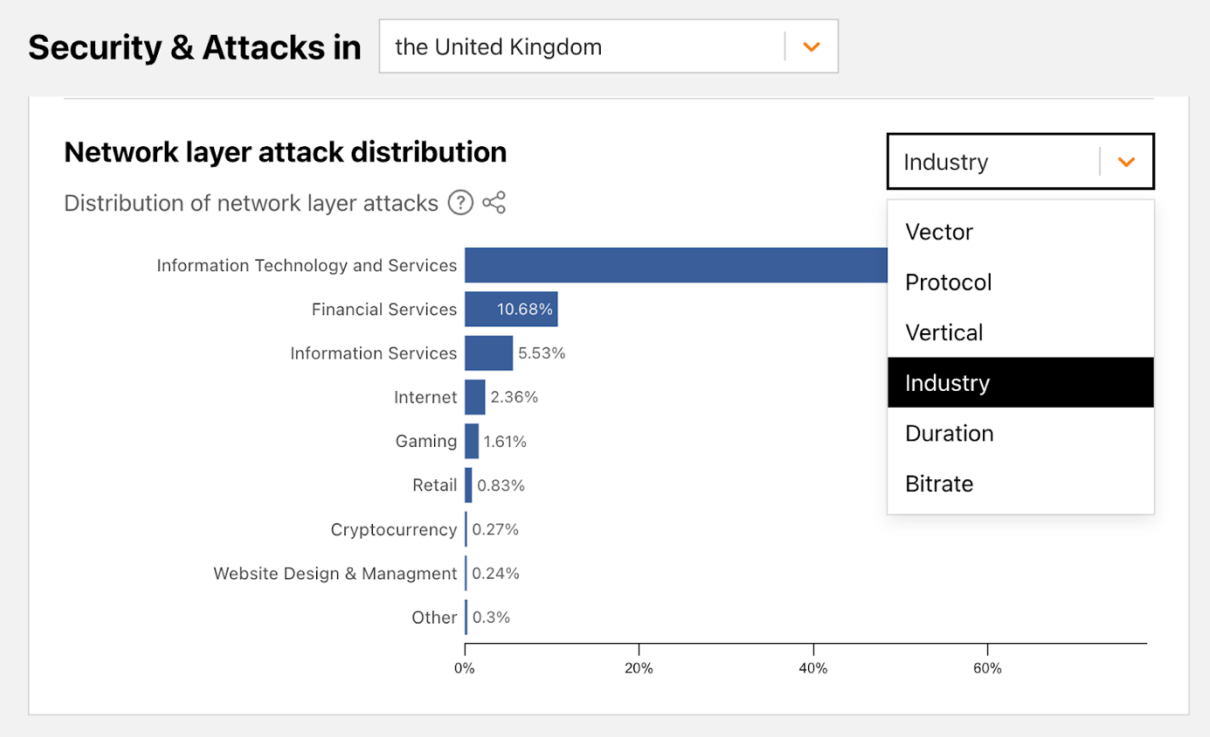
Welcome to the second DDoS threat report of 2023. DDoS attacks, or distributed denial-of-service attacks, are a type of cyber attack that aims to disrupt websites (and other types of Internet properties) to make them unavailable for legitimate users by overwhelming them with more traffic than they can handle — similar to a driver stuck in a traffic jam on the way to the grocery store.

We see a lot of DDoS attacks of all types and sizes and our network is one of the largest in the world spanning more than 300 cities in over 100 countries. Through this network we serve over 63 million HTTP requests per second at peak and over 2 trillion DNS queries every day. This colossal amount of data gives us a unique vantage point to provide the community access to insightful DDoS trends.

For our regular readers, you might notice a change in the layout of this report. We used to follow a set pattern to share our insights and trends about DDoS attacks. But with the landscape of DDoS threats changing as

DDoS attacks have become more powerful and sophisticated, we felt it's time for a change in how we present our findings. So, we'll kick things off with a quick global overview, and then dig into the major shifts we're seeing in the world of DDoS attacks.

Reminder: an interactive version of this report is also available on Cloudflare Radar. Furthermore, we've also added a new interactive component that will allow you to dive deeper into attack activity in each country or region.



New interactive Radar graph to shed light on local DDoS activity

The DDoS landscape: a look at global patterns

The second quarter of 2023 was characterized by thought-out, tailored and persistent waves of DDoS attack campaigns on various fronts, including:

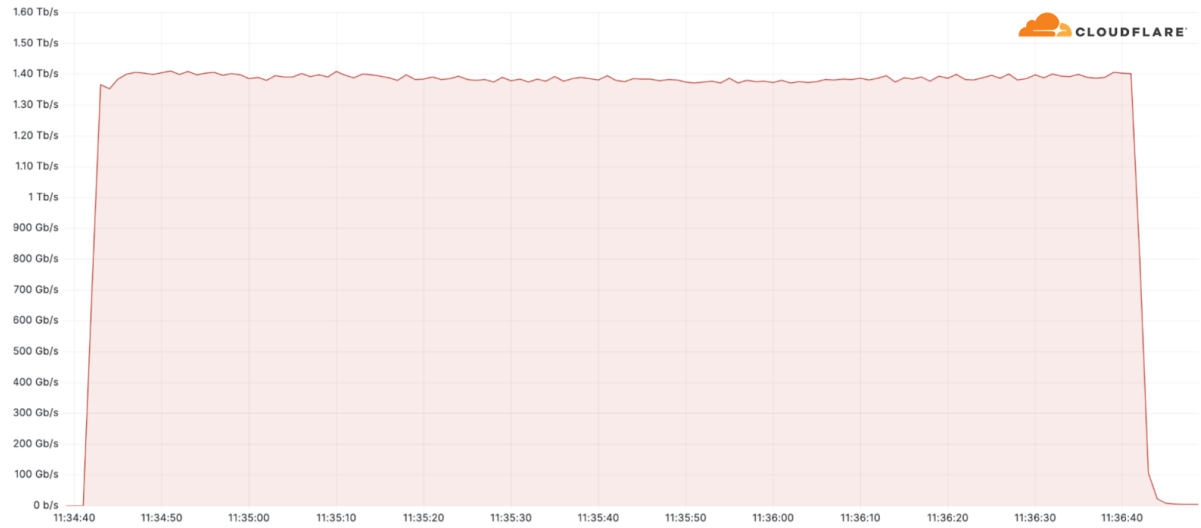
1. Multiple DDoS offensives orchestrated by pro-Russian hacktivist groups REvil, Killnet and Anonymous Sudan against Western interest websites.

2. An increase in deliberately engineered and targeted DNS attacks alongside a 532% surge in DDoS attacks exploiting the Mitel vulnerability (CVE-2022-26143). Cloudflare contributed to disclosing this zero-day vulnerability last year.
3. Attacks targeting Cryptocurrency companies increased by 600%, as a broader 15% increase in HTTP DDoS attacks was observed. Of these, we've noticed an alarming escalation in attack sophistication which we will cover more in depth.

Additionally, one of the largest attacks we've seen this quarter was an ACK flood DDoS attack which originated from a Mirai-variant botnet comprising approximately 11K IP addresses. The attack targeted an American Internet Service Provider. It peaked at 1.4 terabit per seconds (Tbps) and was automatically detected and mitigated by Cloudflare's systems.

Despite general figures indicating an increase in overall attack durations, most of the attacks are short-lived and so was this one. This attack lasted only two minutes. However, more broadly, we've seen that **attacks exceeding 3 hours have increased by 103% QoQ.**

Now having set the stage, let's dive deeper into these shifts we're seeing in the DDoS landscape.

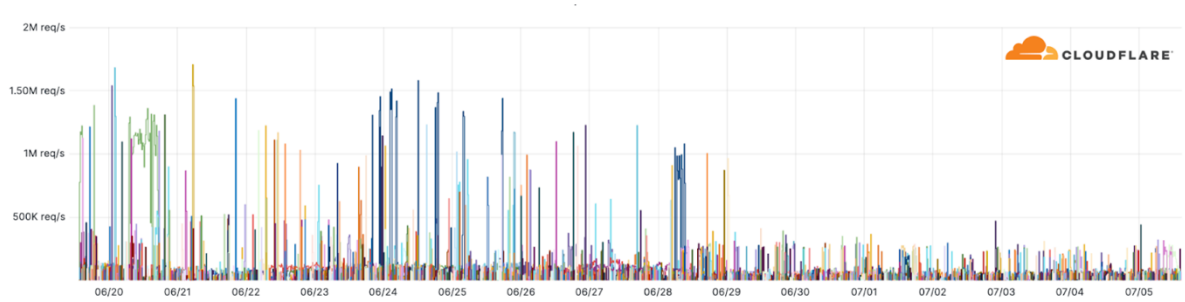


Mirai botnet attacks an American Service Provider, peaks at 1.4 Tbps

Hacktivist alliance dubbed “Darknet Parliament” aims at Western banks and SWIFT network

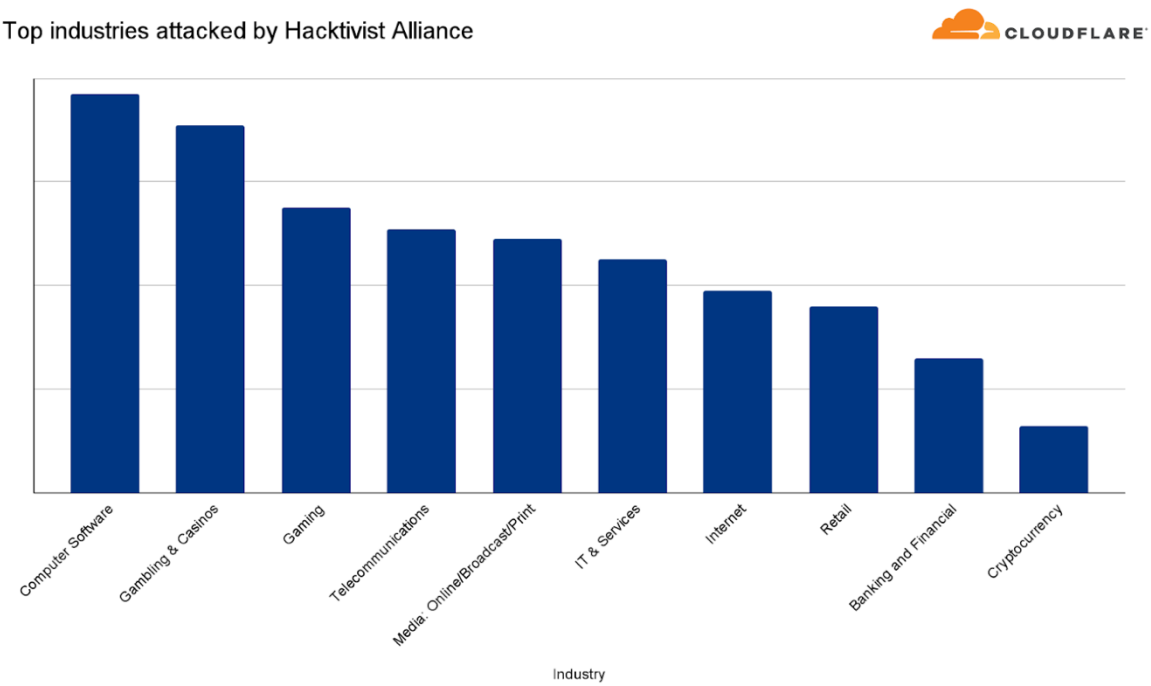
On June 14, Pro-Russian hacktivist groups Killnet, a resurgence of REvil and Anonymous Sudan announced that they have joined forces to execute “massive” cyber attacks on the Western financial system including European and US banks, and the US Federal Reserve System. The collective, dubbed “Darknet Parliament”, declared its first objective was to paralyze SWIFT (Society for Worldwide Interbank Financial Telecommunication). A successful DDoS attack on SWIFT could have dire consequences because it's the main service used by financial institutions to conduct global financial transactions.

Beyond a handful of publicized events such as the Microsoft outage which was reported by the media, we haven’t observed any novel DDoS attacks or disruptions targeting our customers. Our systems have been automatically detecting and mitigating attacks associated with this campaign. Over the past weeks, as many as 10,000 of these DDoS attacks were launched by the Darknet Parliament against Cloudflare-protected websites (see graph below).



REvil, Killnet and Anonymous Sudan attacks

Despite the hacktivists’ statements, Banking and Financial Services websites were only the ninth most attacked industry — based on attacks we’ve seen against our customers as part of this campaign.



Top industries attacked by the REvil, Killnet and Anonymous Sudan attack campaign

The most attacked industries were Computer Software, Gambling & Casinos and Gaming. Telecommunications and Media outlets came in fourth and fifth, respectively. Overall, the largest attack we witnessed in this campaign peaked at 1.7 million requests per second (rps) and the average was 65,000 rps.

For perspective, earlier this year we mitigated the largest attack in recorded history peaking at 71 million rps. So these attacks were very small compared to *Cloudflare scale*, but not necessarily for an average website. Therefore, we shouldn't underestimate the damage potential on unprotected or suboptimally configured websites.

Sophisticated HTTP DDoS attacks

An HTTP DDoS attack is a DDoS attack over the Hypertext Transfer Protocol (HTTP). It targets HTTP Internet properties such as websites and API gateways. Over the past quarter, HTTP DDoS attacks increased by 15% quarter-over-quarter (QoQ) despite a 35% decrease year-over-year (YoY).

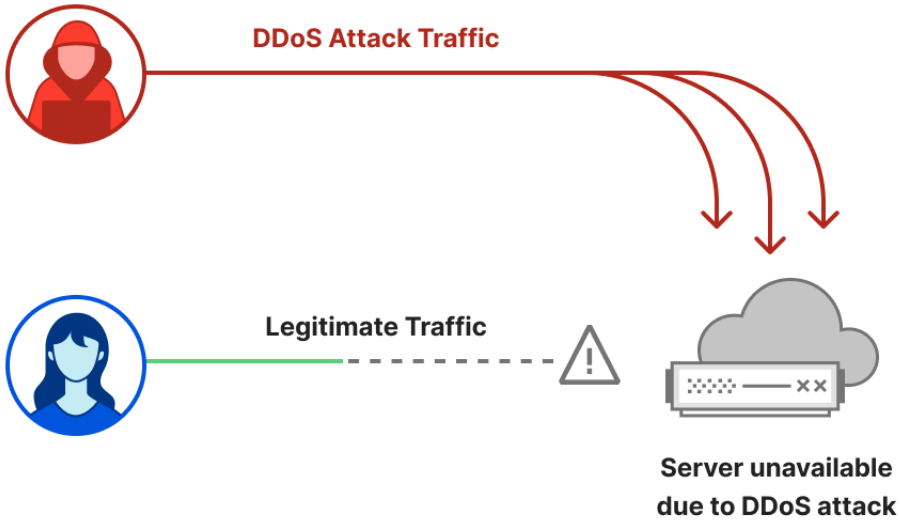
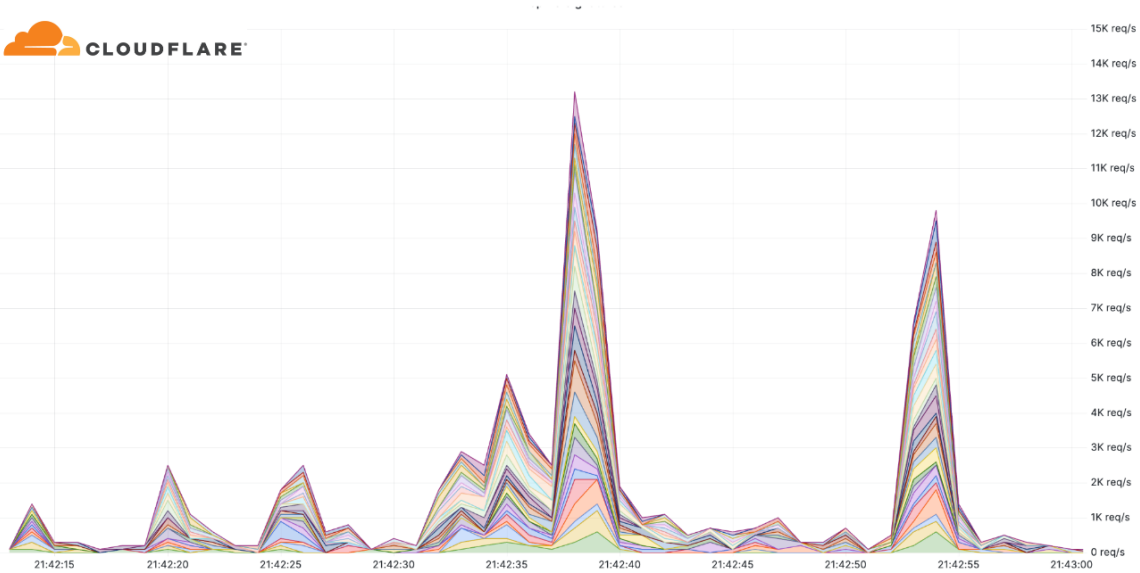


Illustration of an HTTP DDoS attack

Additionally, we've observed an alarming uptick in highly-randomized and sophisticated HTTP DDoS attacks over the past few months. It appears as though the threat actors behind these attacks have deliberately engineered the attacks to try and overcome mitigation systems by adeptly imitating browser behavior very accurately, in some cases, by introducing a high degree of randomization on various properties such as user agents and JA3 fingerprints to name a few. An example of such an attack is provided below. Each different color represents a different randomization feature.



Example of a highly randomized HTTP DDoS attack

Furthermore, in many of these attacks, it seems that the threat actors try to keep their attack rates-per-second relatively low to try and avoid detection and hide amongst the legitimate traffic.

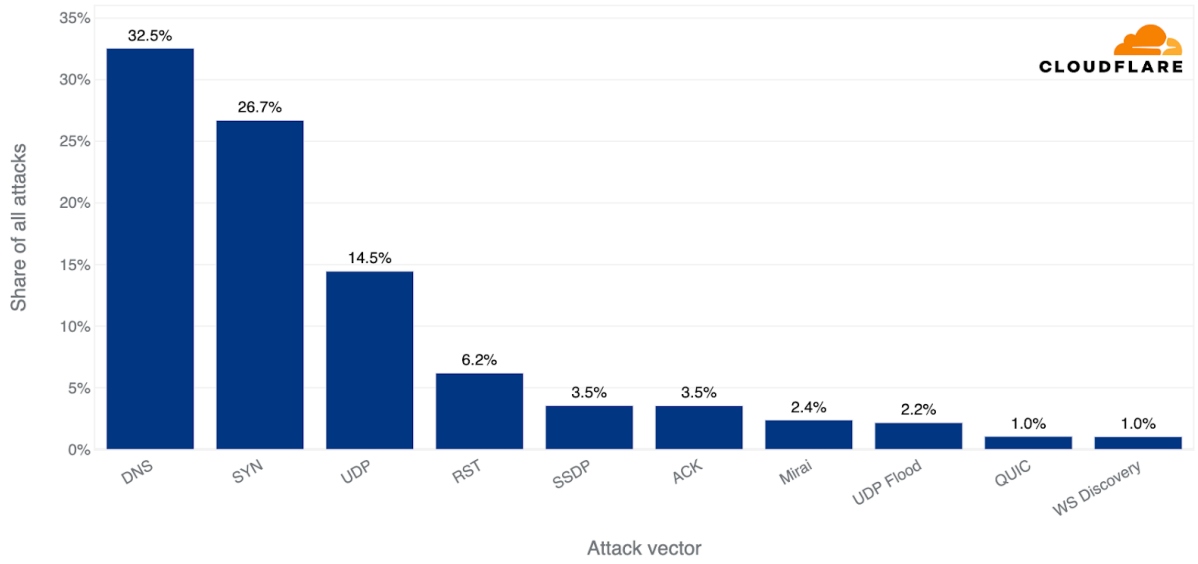
This level of sophistication has previously been associated with state-level and state-sponsored threat actors, and it seems these capabilities are now at the disposal of cyber criminals. Their operations have already targeted prominent businesses such as a large VoIP provider, a leading semiconductor company, and a major payment & credit card provider to name a few.

Protecting websites against sophisticated HTTP DDoS attacks requires intelligent protection that is automated and fast, that leverages threat intelligence, traffic profiling and Machine Learning/statistical analysis to differentiate between attack traffic and user traffic. Moreover, even increasing caching where applicable can help reduce the risk of attack traffic impacting your origin. Read more about DDoS protection best practices here.

DNS Laundering DDoS attacks

The Domain Name System, or DNS, serves as the phone book of the Internet. DNS helps translate the human-friendly website address (e.g. www.cloudflare.com) to a machine-friendly IP address (e.g. 104.16.124.96). By disrupting DNS servers, attackers impact the machines' ability to connect to a website, and by doing so making websites unavailable to users.

Over the past quarter, the most common attack vector was DNS-based DDoS attacks — 32% of all DDoS attacks were over the DNS protocol. Amongst these, one of the more concerning attack types we've seen increasing is the *DNS Laundering attack* which can pose severe challenges to organizations that operate their own authoritative DNS servers.



Top DDoS attack vectors in 2023 Q2

The term “Laundering” in the DNS Laundering attack name refers to the analogy of money laundering, the devious process of making illegally-gained proceeds, often referred to as "dirty money," appear legal. Similarly, in the DDoS world, a DNS Laundering attack is the process of making bad, malicious traffic appear as good, legitimate traffic by laundering it via reputable recursive DNS resolvers.

In a DNS Laundering attack, the threat actor will query subdomains of a domain that is managed by the victim’s DNS server. The prefix that defines the subdomain is randomized and is never used more than once or twice in such an attack. Due to the randomization element, recursive DNS servers will never have a cached response and will need to forward the query to the victim’s authoritative DNS server. The authoritative DNS server is then bombarded by so many queries until it cannot serve legitimate queries or even crashes all together.

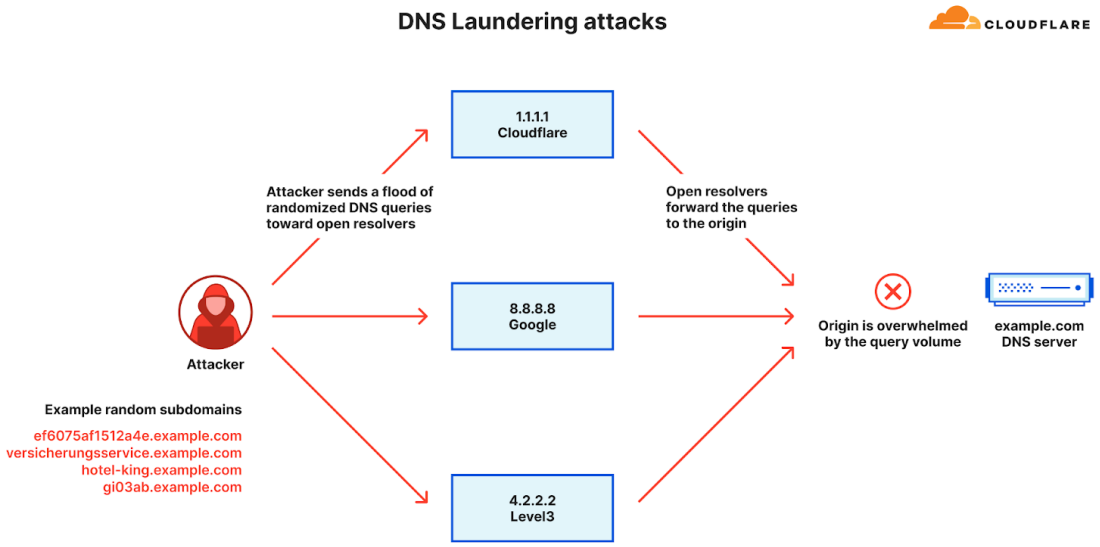
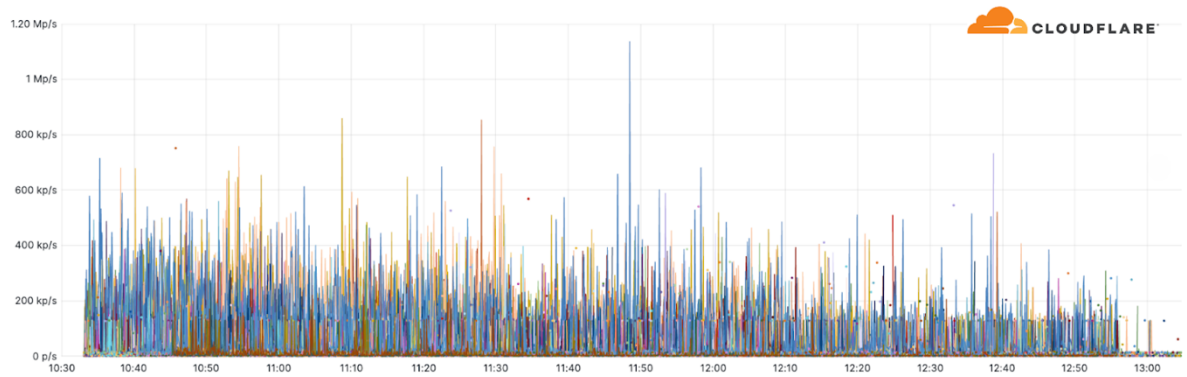


Illustration of a DNS Laundering DDoS attack

From the protection point of view, the DNS administrators can't block the attack source because the source includes reputable recursive DNS servers like Google's 8.8.8.8 and Cloudflare's 1.1.1.1. The administrators also cannot block all queries to the attacked domain because it is a valid domain that they want to preserve access to legitimate queries.

The above factors make it very challenging to distinguish legitimate queries from malicious ones. A large Asian financial institution and a North American DNS provider are amongst recent victims of such attacks. An example of such an attack is provided below.



Example of a DNS Laundering DDoS attack

Similar to the protection strategies outlined for HTTP applications, protecting DNS servers also requires a precise, fast, and automated

approach. Leveraging a managed DNS service or a DNS reverse proxy such as Cloudflare's can help absorb and mitigate the attack traffic. For those more sophisticated DNS attacks, a more intelligent solution is required that leverages statistical analysis of historical data to be able to differentiate between legitimate queries and attack queries.

The rise of the Virtual Machine Botnets

As we've previously disclosed, we are witnessing an evolution in botnet *DNA*. The era of VM-based DDoS botnets has arrived and with it *hyper-volumetric* DDoS attacks. These botnets are comprised of Virtual Machines (VMs, or Virtual Private Servers, VPS) rather than Internet of Things (IoT) devices which makes them so much more powerful, up to 5,000 times stronger.

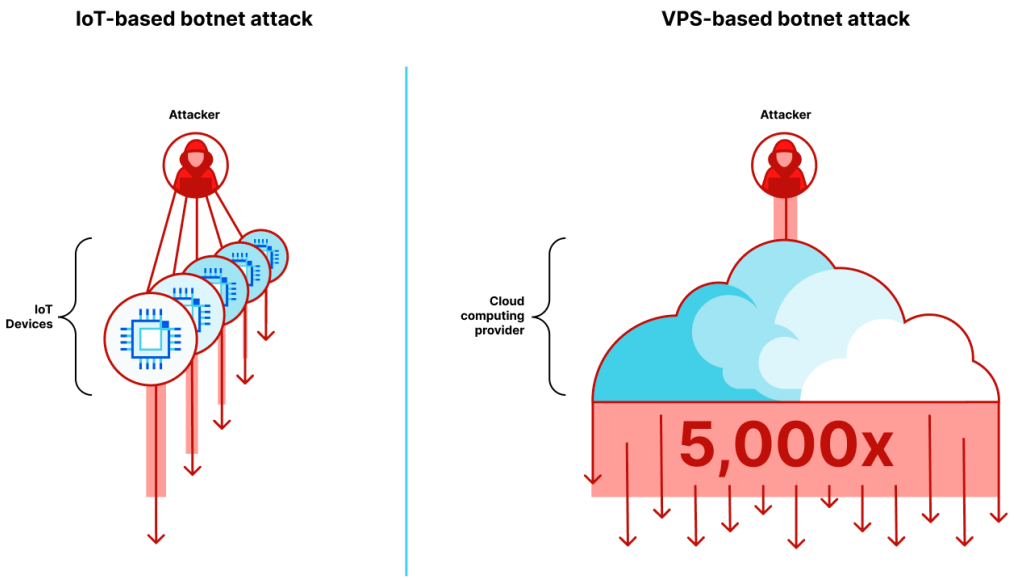
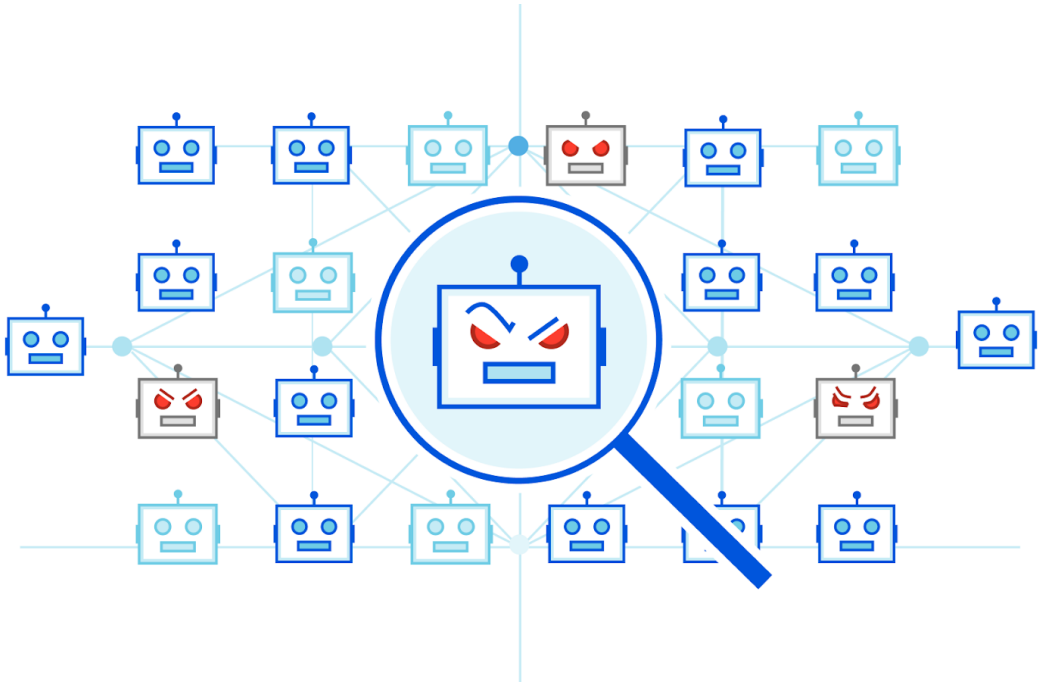


Illustration of an IoT botnet compared with a VM Botnet

Because of the computational and bandwidth resources that are at the disposal of these VM-based botnets, they're able to generate hyper-volumetric attacks with a much smaller fleet size compared to IoT-based botnets.

These botnets have executed one largest recorded DDoS attacks including the 71 million request per second DDoS attack. Multiple organizations including an industry-leading gaming platform provider have already been targeted by this new generation of botnets.



Cloudflare has proactively collaborated with prominent cloud computing providers to combat these new botnets. Through the quick and dedicated actions of these providers, significant components of these botnets have been neutralized. Since this intervention, we have not observed any further hyper-volumetric attacks yet, a testament to the efficacy of our collaboration.

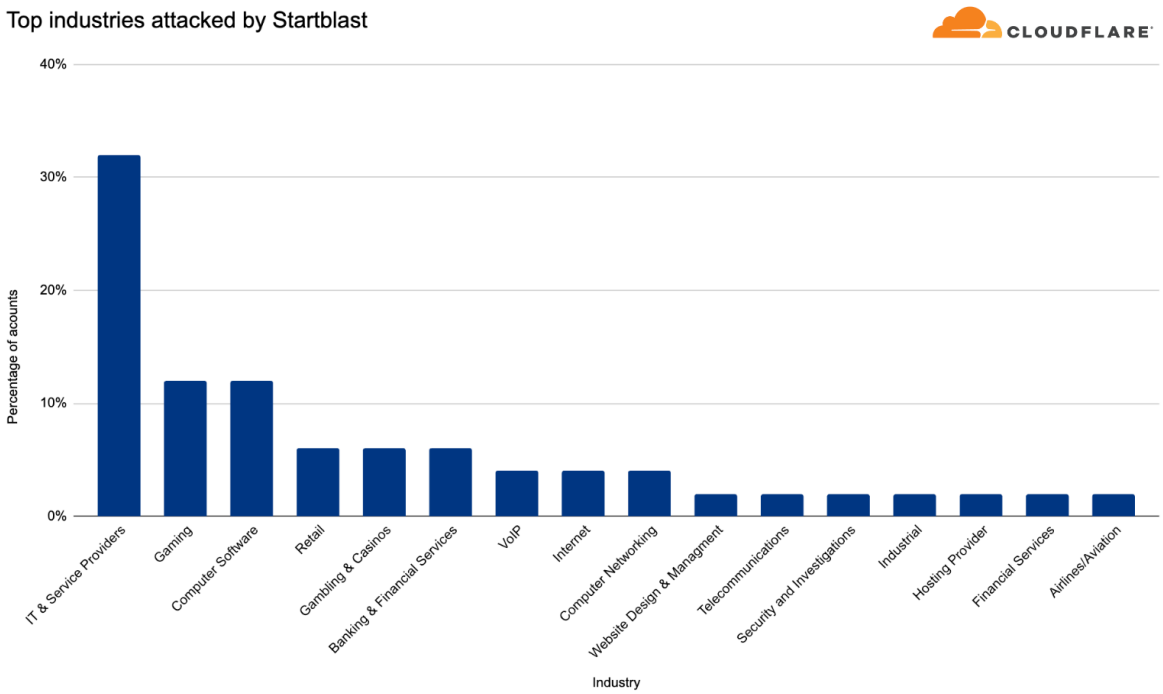
While we already enjoy a fruitful alliance with the cybersecurity community in countering botnets when we identify large-scale attacks, our goal is to streamline and automate this process further. We extend an invitation to cloud computing providers, hosting providers, and other general service providers to join Cloudflare's free Botnet Threat Feed. This would provide visibility into attacks originating within their networks, contributing to our collective efforts to dismantle botnets.

"Startblast": Exploiting Mitel vulnerabilities for DDoS attacks

In March 2022, we disclosed a zero-day vulnerability (CVE-2022-26143), named TP240PhoneHome, which was identified in the Mitel MiCollab business phone system, exposing the system to UDP amplification DDoS attacks.

This exploit operates by reflecting traffic off vulnerable servers, amplifying it in the process, with a factor as high as 220 billion percent. The vulnerability stems from an unauthenticated UDP port exposed to the public Internet, which could allow malicious actors to issue a 'startblast' debugging command, simulating a flurry of calls to test the system.

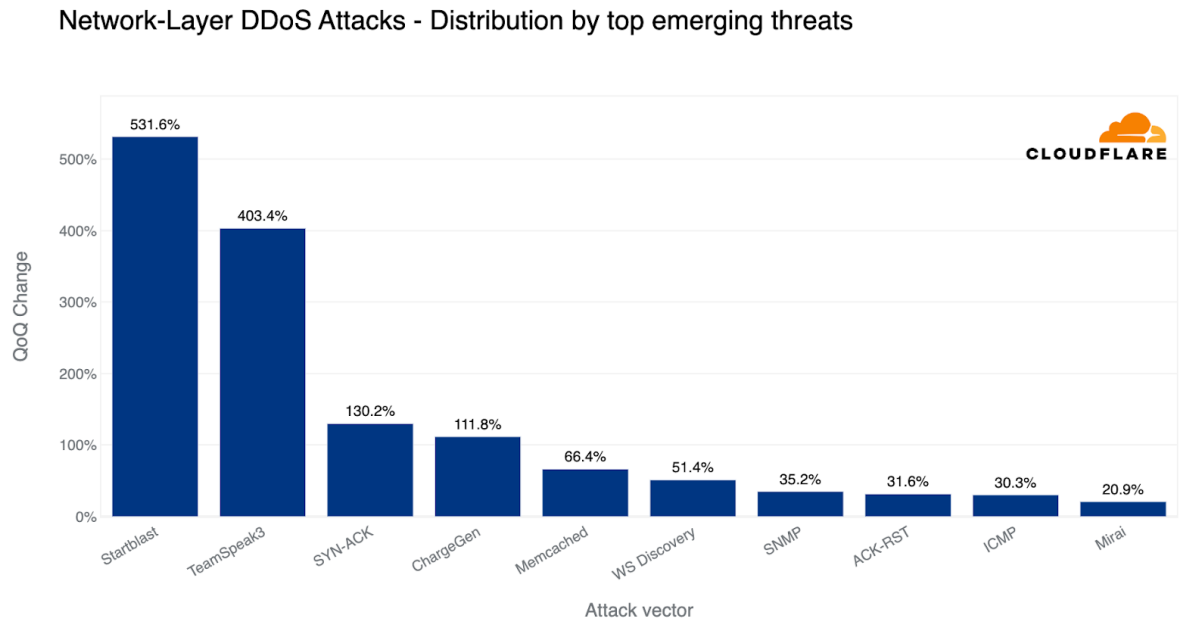
As a result, for each test call, two UDP packets are sent to the issuer, enabling an attacker to direct this traffic to any IP and port number to amplify a DDoS attack. Despite the vulnerability, only a few thousand of these devices are exposed, limiting the potential scale of attack, and attacks must run serially, meaning each device can only launch one attack at a time.



Top industries targeted by Startblast DDoS attacks

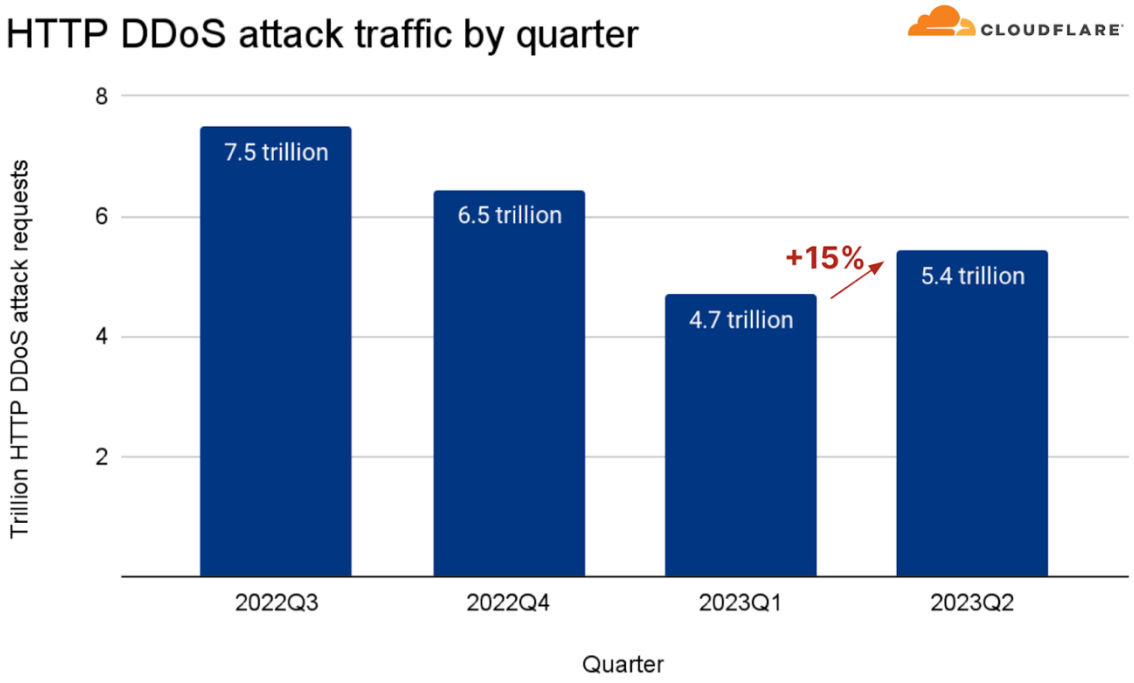
Overall, in the past quarter, we've seen additional emerging threats such as DDoS attacks abusing the TeamSpeak3 protocol. This attack vector increased by a staggering 403% this quarter.

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



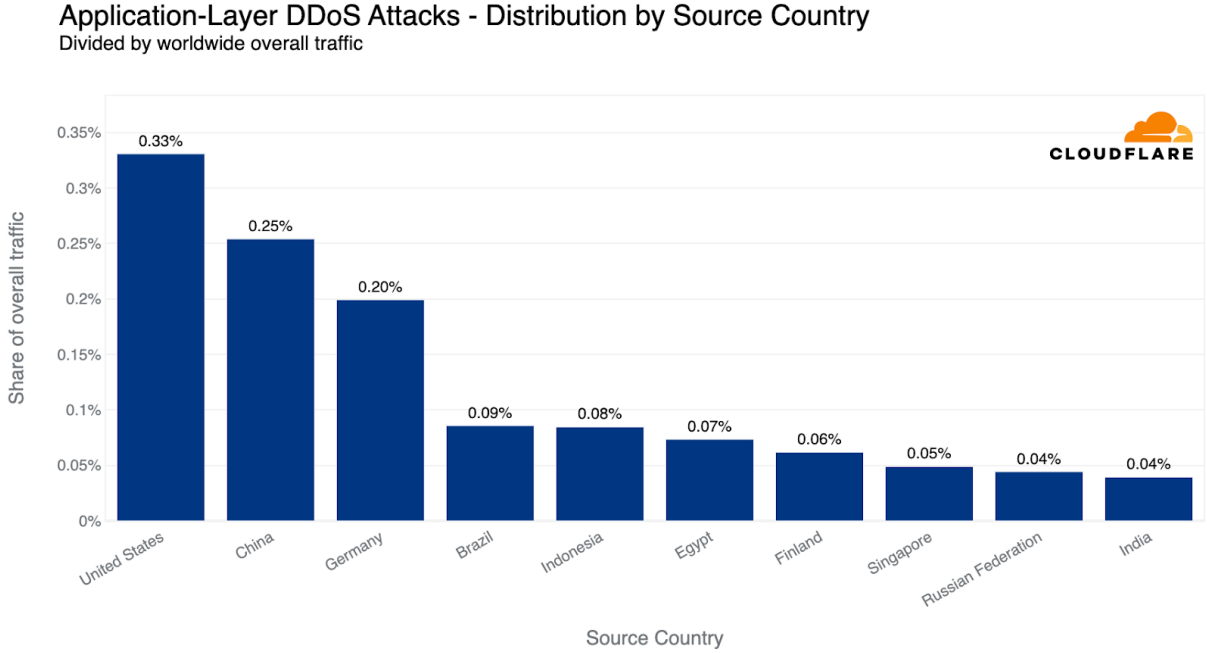
DDoS hotspots: The origins of attacks

Overall, HTTP DDoS attacks increased by 15% QoQ despite a 35% decrease YoY. Additionally, network-layer DDoS attacks decreased this quarter by approximately 14%.



HTTP DDoS attack requests by quarter

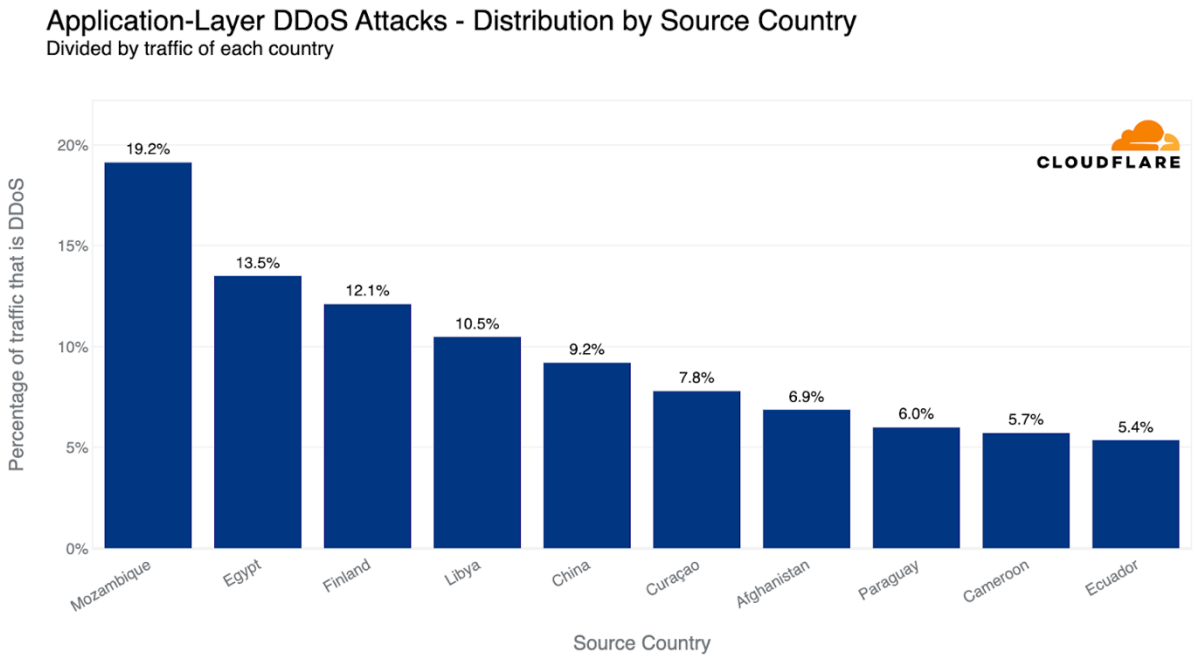
In terms of total volume of attack traffic, the US was the largest source of HTTP DDoS attacks. Three out of every thousand requests we saw were part of HTTP DDoS attacks originating from the US. China came in second place and Germany in third place.



Top source countries of HTTP DDoS attacks (percentage of attack traffic out of the total traffic worldwide)

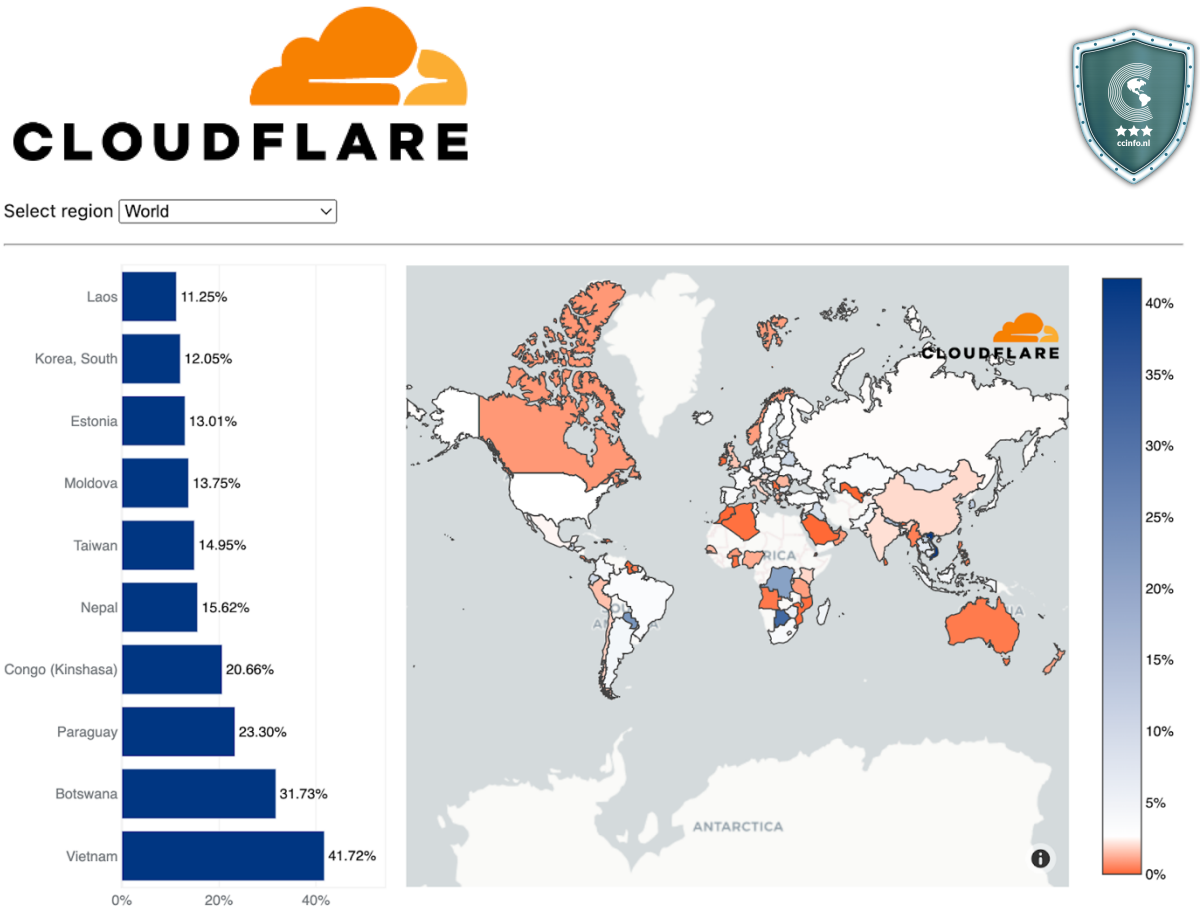
Some countries naturally receive more traffic due to various factors such as market size, and therefore more attacks. So while it's interesting to understand the total amount of attack traffic originating from a given country, it is also helpful to remove that bias by normalizing the attack traffic by all traffic to a given country.

When doing so, we see a different pattern. The US doesn't even make it into the top ten. Instead, Mozambique, Egypt and Finland take the lead as the source countries of the most HTTP DDoS attack traffic relative to all of their traffic. Almost a fifth of all HTTP traffic originating from Mozambique IP addresses were part of DDoS attacks.



Top source countries of HTTP DDoS attacks (percentage of attack traffic out of the total traffic per country)

Using the same calculation methodology but for bytes, Vietnam remains the largest source of network-layer DDoS attacks (aka L3/4 DDoS attacks) for the second consecutive quarter — and the amount even increased by 58% QoQ. Over 41% of all bytes that were ingested in Cloudflare's Vietnam data centers were part of L3/4 DDoS attacks.

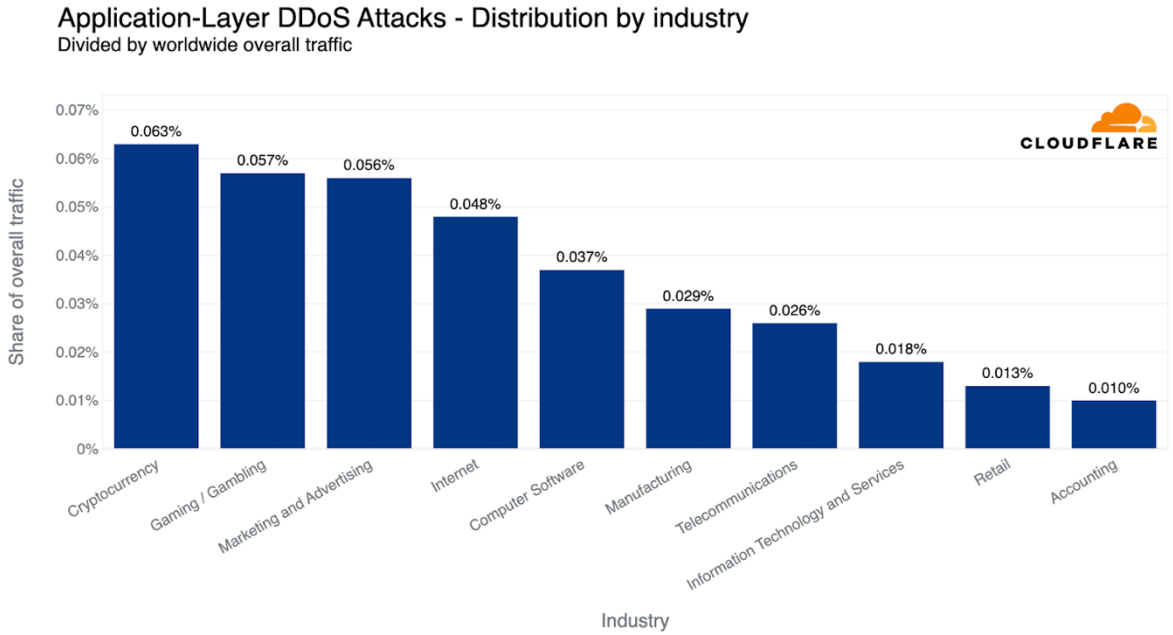


Top source countries of L3/4 DDoS attacks (percentage of attack traffic out of the total traffic per country)

Industries under attack: examining DDoS attack targets

When examining HTTP DDoS attack activity in Q2, Cryptocurrency websites were targeted with the largest amount of HTTP DDoS attack traffic. Six out of every ten thousand HTTP requests towards Cryptocurrency websites behind Cloudflare were part of these attacks. This represents a 600% increase compared to the previous quarter.

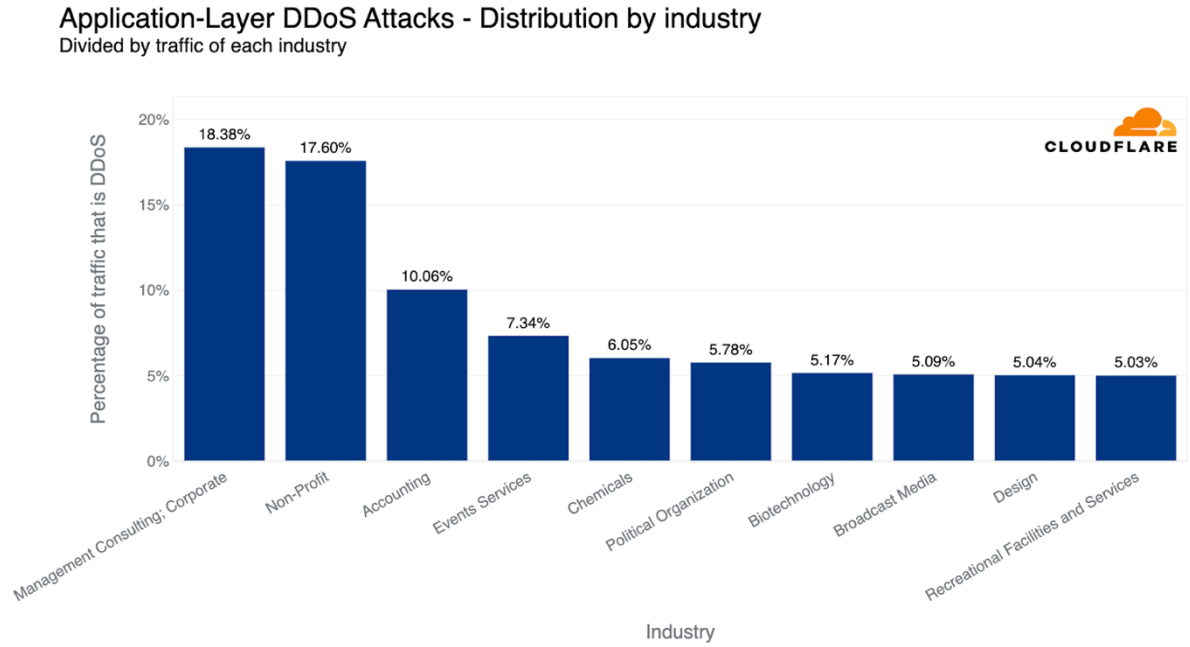
After Crypto, Gaming and Gambling websites came in second place as their attack share increased by 19% QoQ. Marketing and Advertising websites not far behind in third place with little change in their share of attacks.



Top industries targeted by HTTP DDoS attacks (percentage of attack traffic out of the total traffic for all industries)

However, when we look at the amount of attack traffic relative to all traffic for any given industry, the numbers paint a different picture. Last quarter, Non-profit organizations were attacked the most — 12% of traffic to Non-profits were HTTP DDoS attacks. Cloudflare protects more than 2,271 Non-profit organizations in 111 countries as part of Project Galileo which celebrated its ninth anniversary this year. Over the past months, an average of 67.7 million cyber attacks targeted Non-profits on a daily basis.

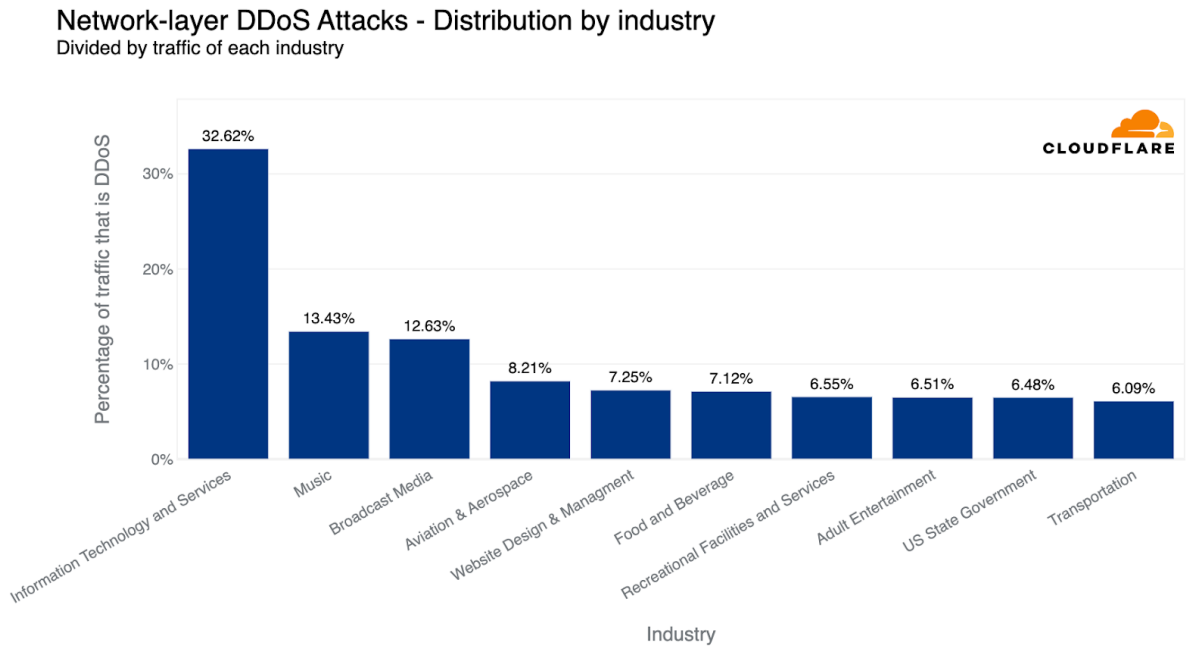
Overall, the amount of DDoS attacks on Non-profits increased by 46% bringing the percentage of attack traffic to 17.6%. However, despite this growth, the Management Consulting industry jumped to the first place with 18.4% of its traffic being DDoS attacks.



Top industries targeted by HTTP DDoS attacks (percentage of attack traffic out of the total traffic per industry)

When descending the layers of the OSI model, the Internet networks that were most targeted belonged to the Information Technology and Services industry. Almost every third byte routed to them were part of L3/4 DDoS attacks.

Surprisingly enough, companies operating in the Music industry were the second most targeted industry, followed by Broadcast Media and Aviation & Aerospace.



Top industries targeted by L3/4 DDoS attacks (percentage of attack traffic out of the total traffic per industry)

Top attacked industries: a regional perspective

Cryptocurrency websites experienced the highest number of attacks worldwide, while Management Consulting and Non-profit sectors were the most targeted considering their total traffic. However, when we look at individual regions, the situation is a bit different.

Top industries targeted by HTTP DDoS attacks by region

Africa

The Telecommunications industry remains the most attacked industry in Africa for the second consecutive quarter. The Banking, Financial Services and Insurance (BFSI) industry follows as the second most attacked. The majority of the attack traffic originated from Asia (35%) and Europe (25%).

Asia

For the past two quarters, the Gaming and Gambling industry was the most targeted industry in Asia. In Q2, however, the Gaming and Gambling industry dropped to second place and Cryptocurrency took the lead as the most attacked industry (~50%). Substantial portions of the attack traffic originated from Asia itself (30%) and North America (30%).

Europe

For the third consecutive quarter, the Gaming & Gambling industry remains the most attacked industry in Europe. The Hospitality and Broadcast Media industries follow not too far behind as the second and

third most attacked. Most of the attack traffic came from within Europe itself (40%) and from Asia (20%).

Latin America

Surprisingly, half of all attack traffic targeting Latin America was aimed at the Sporting Goods industry. In the previous quarter, the BFSI was the most attacked industry. Approximately 35% of the attack traffic originated from Asia, and another 25% originated from Europe.

Middle East

The Media & Newspaper industries were the most attacked in the Middle East. The vast majority of attack traffic originated from Europe (74%).

North America

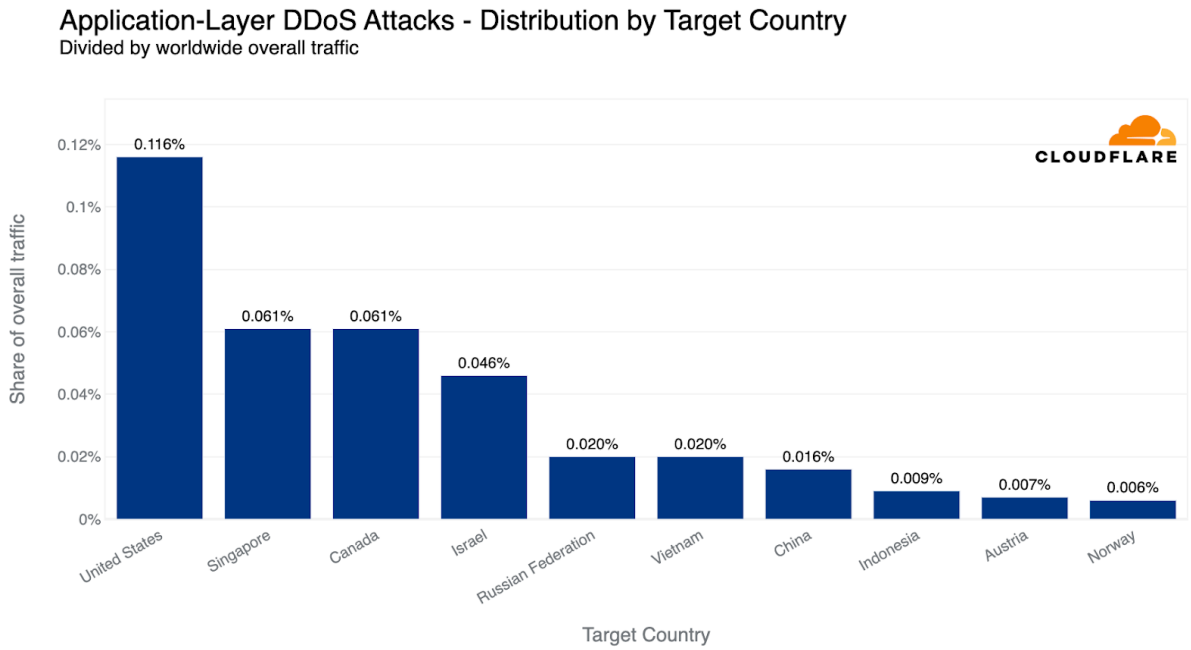
For the second consecutive quarter, Marketing & Advertising companies were the most attacked in North America (approximately 35%). Manufacturing and Computer Software companies came in second and third places, respectively. The main sources of the attack traffic were Europe (42%) and the US itself (35%).

Oceania

This quarter, the Biotechnology industry was the most attacked. Previously, it was the Health & Wellness industry. Most of the attack traffic originated from Asia (38%) and Europe (25%).

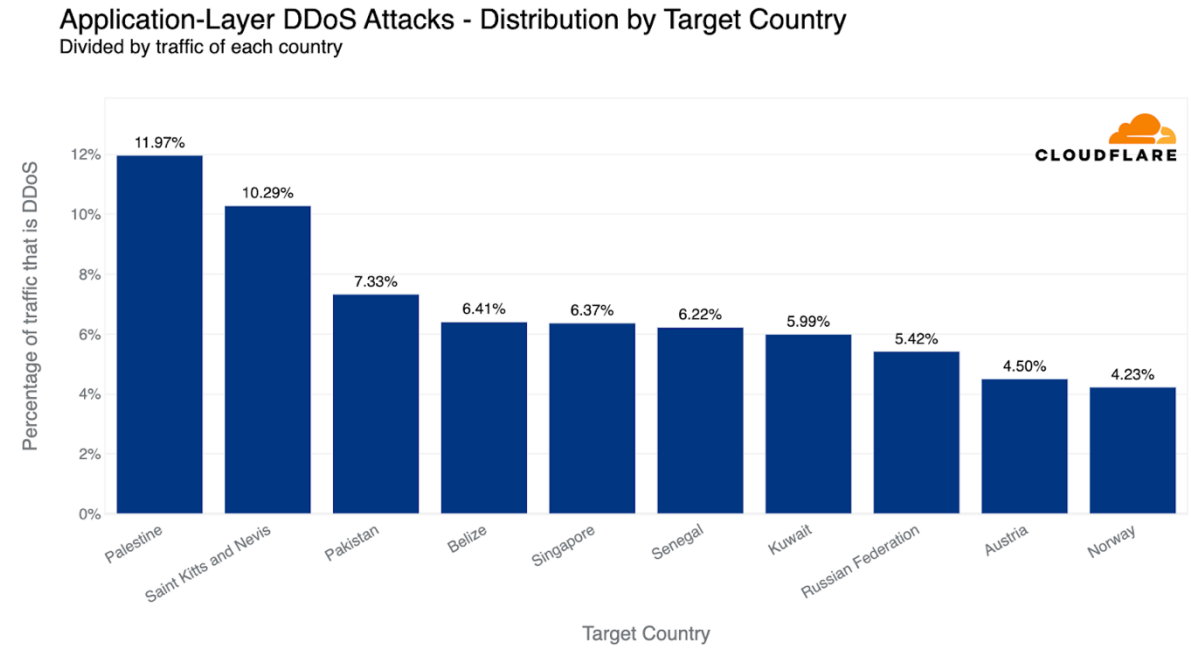
Countries and regions under attack: examining DDoS attack targets

When examining the total volume of attack traffic, last quarter, Israel leaped to the front as the most attacked country. This quarter, attacks targeting Israeli websites decreased by 33% bringing it to the fourth place. The US takes the lead again as the most attacked country, followed by Canada and Singapore.



Top countries and regions targeted by HTTP DDoS attacks (percentage of attack traffic out of the total traffic for all countries and regions)

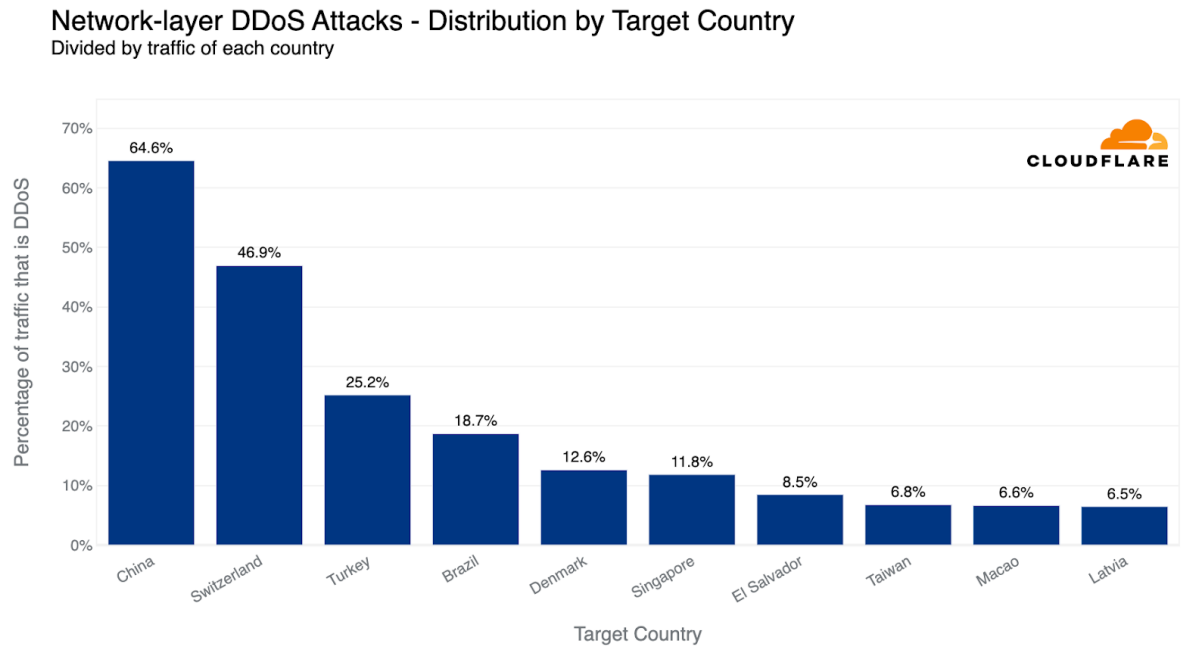
If we normalize the data per country and region and divide the attack traffic by the total traffic, we get a different picture. Palestine jumps to the first place as the most attacked country. Almost 12% of all traffic to Palestinian websites were HTTP DDoS attacks.



Top countries and regions targeted by HTTP DDoS attacks (percentage of attack traffic out of the total traffic per country and region)

Last quarter, we observed a striking deviation at the network layer, with Finnish networks under Cloudflare's shield emerging as the primary target. This surge was likely correlated with the diplomatic talks that precipitated Finland's formal integration into NATO. Roughly 83% of all incoming traffic to Finland comprised cyberattacks, with China a close second at 68% attack traffic.

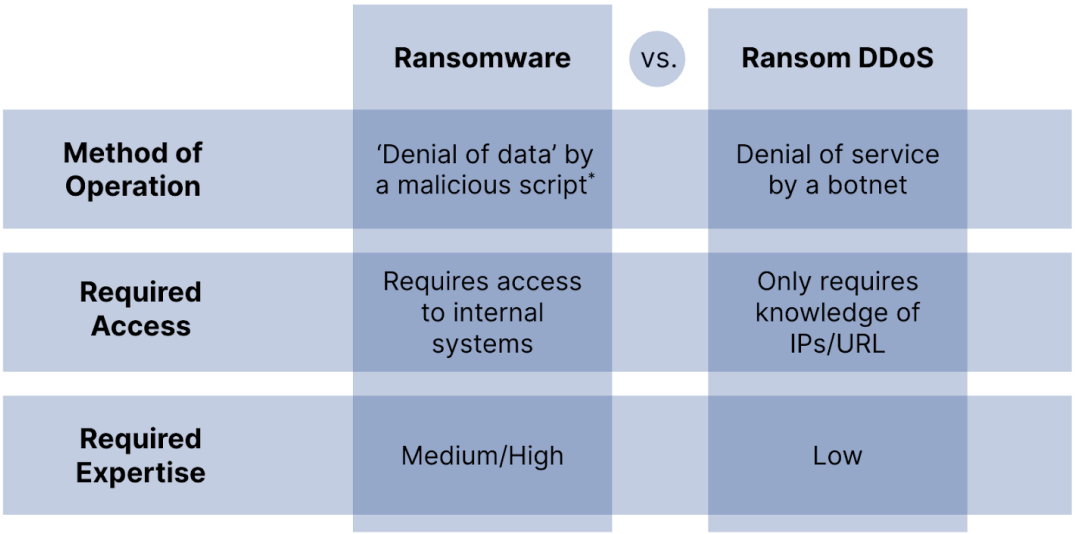
This quarter, however, paints a very different picture. Finland has receded from the top ten, and Chinese Internet networks behind Cloudflare have ascended to the first place. Almost two-thirds of the byte streams towards Chinese networks protected by Cloudflare were malicious. Following China, Switzerland saw half of its inbound traffic constituting attacks, and Turkey came third, with a quarter of its incoming traffic identified as hostile.



Top countries and regions targeted by L3/4 DDoS attacks (percentage of attack traffic out of the total traffic per country and region)

Ransom DDoS attacks

Occasionally, DDoS attacks are carried out to extort ransom payments. We've been surveying Cloudflare customers over three years now, and have been tracking the occurrence of Ransom DDoS attack events.



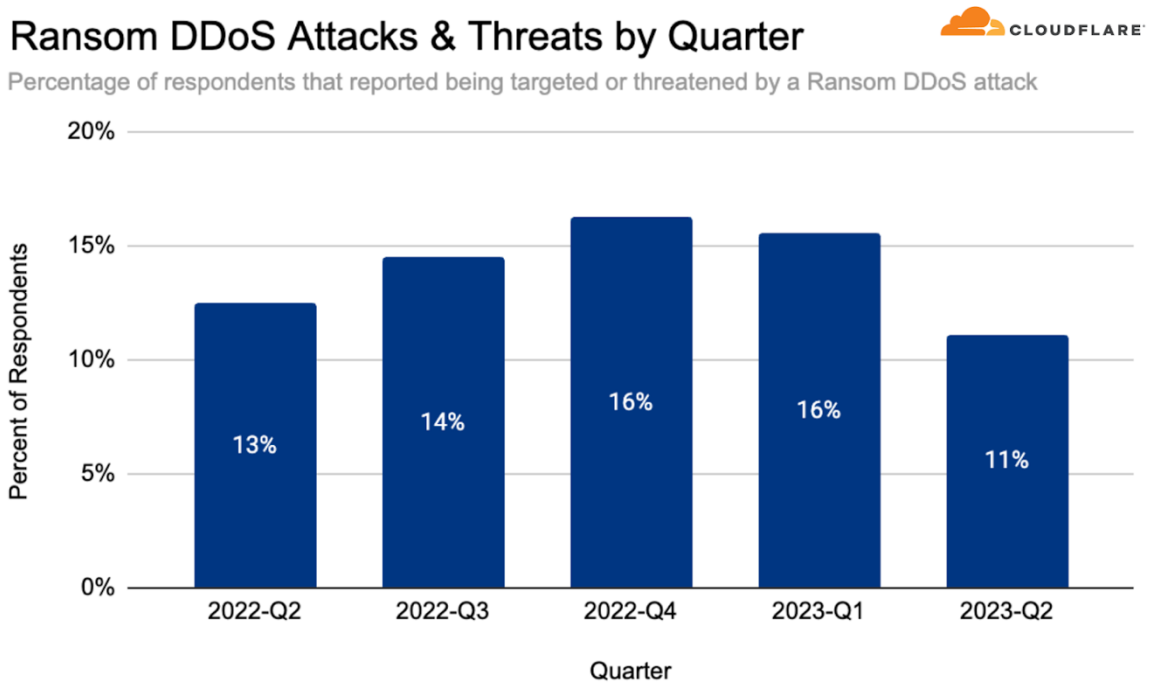
	Ransomware	vs.	Ransom DDoS
Method of Operation	'Denial of data' by a malicious script*		Denial of service by a botnet
Required Access	Requires access to internal systems		Only requires knowledge of IPs/URL
Required Expertise	Medium/High		Low

* More specifically, Malware or Ransomware can be used to encrypt, leak or delete the victim's data.

High level comparison of Ransomware and Ransom DDoS attacks

Unlike Ransomware attacks, where victims typically fall prey to downloading a malicious file or clicking on a compromised email link which locks, deletes or leaks their files until a ransom is paid, Ransom DDoS attacks can be much simpler for threat actors to execute. Ransom DDoS attacks bypass the need for deceptive tactics such as luring victims into opening dubious emails or clicking on fraudulent links, and they don't necessitate a breach into the network or access to corporate resources.

Over the past quarter, reports of Ransom DDoS attacks decreased. One out of ten respondents reported being threatened or subject to Ransom DDoS attacks.



Wrapping up: the ever-evolving DDoS threat landscape

In recent months, there's been an alarming escalation in the sophistication of DDoS attacks. And even the largest and most sophisticated attacks that we've seen may only last a few minutes or even seconds — which doesn't give a human sufficient time to respond. Before the PagerDuty alert is even sent, the attack may be over and the damage is done. Recovering from a DDoS attack can last much longer than the attack itself — just as a boxer might need a while to recover from a punch to the face that only lasts a fraction of a second.

Security is not one single product or a click of a button, but rather a process involving multiple layers of defense to reduce the risk of impact. Cloudflare's automated DDoS defense systems consistently safeguard our clients from DDoS attacks, freeing them up to focus on their core business operations. These systems are complemented by the vast breadth of Cloudflare capabilities such as firewall, bot detection, API protection and even caching which can all contribute to reducing the risk of impact.

The DDoS threat landscape is evolving and increasingly complex, demanding more than just quick fixes. Thankfully, with Cloudflare's multi-

layered defenses and automatic DDoS protections, our clients are equipped to navigate these challenges confidently. Our mission is to help build a better Internet, and so we continue to stand guard, ensuring a safer and more reliable digital realm for all.

Methodologies

How we calculate Ransom DDoS attack insights

Cloudflare's systems constantly analyze traffic and automatically apply mitigation when DDoS attacks are detected. Each attacked customer is prompted with an automated survey to help us better understand the nature of the attack and the success of the mitigation. For over two years, Cloudflare has been surveying attacked customers. One of the questions in the survey asks the respondents if they received a threat or a ransom note. Over the past two years, on average, we collected 164 responses per quarter. The responses of this survey are used to calculate the percentage of Ransom DDoS attacks.

How we calculate geographical and industry insights

Source country
At the application-layer, we use the attacking IP addresses to understand the origin country of the attacks. That is because at that layer, IP addresses cannot be spoofed (i.e., altered). However, at the network layer, source IP addresses can be spoofed. So, instead of relying on IP addresses to understand the source, we instead use the location of our data centers where the attack packets were ingested. We're able to get geographical accuracy due to our large global coverage in over 285 locations around the world.

Target country
For both application-layer and network-layer DDoS attacks, we group attacks and traffic by our customers' billing country. This lets us understand which countries are subject to more attacks.

Target industry
For both application-layer and network-layer DDoS attacks, we group

attacks and traffic by our customers' industry according to our customer relations management system. This lets us understand which industries are subject to more attacks.

Total volume vs. percentage
For both source and target insights, we look at the total volume of attack traffic compared to all traffic as one data point. Additionally, we also look at the percentage of attack traffic towards or from a specific country, to a specific country or to a specific industry. This gives us an "attack activity rate" for a given country/industry which is normalized by their total traffic levels. This helps us remove biases of a country or industry that normally receives a lot of traffic and therefore a lot of attack traffic as well.

How we calculate attack characteristics
To calculate the attack size, duration, attack vectors and emerging threats, we bucket attacks and then provide the share of each bucket out of the total amount for each dimension. On the new Radar component, these trends are calculated by number of bytes instead. Since attacks may vary greatly in number of bytes from one another, this could lead to trends differing between the reports and the Radar component.

General disclaimer and clarification

When we describe 'top countries' as the source or target of attacks, it does not necessarily mean that that country was attacked as a country, but rather that organizations that use that country as their billing country were targeted by attacks. Similarly, attacks originating from a country does not mean that that country launched the attacks, but rather that the attack was launched from IP addresses that have been mapped to that country. Threat actors operate global botnets with nodes all over the world, and in many cases also use Virtual Private Networks and proxies to obfuscate their true location. So if anything, the source country could indicate the presence of exit nodes or botnet nodes within that country.