Q1 2023 in Review: DDoS Attacks Report by StormWall

StormWall, a global DDoS protection provider, examined Q1 2023 attacks on clients in the financial industry, e-commerce, telecom, entertainment, transport, education, and logistics for its first 2023 report.

Looking back at Q1 2023

Q1 2023 saw a 47% surge in attacks compared to the same period last year, with a shift towards botnet usage and growing instances of smokescreening to hide multi-vector incidents — attacks used as decoy increased by 28% compared to Q1 2022.

Threat actors also began shifting focus to vital infrastructure and services, including logistical services, payment processing hubs, and banking systems, aiming to impact a larger number of users.

The focus on targeting critical infrastructure — which is usually well-hardened — meant that cybercriminals had to further increase their firepower. On average, the **attacks we recorded peaked at 1.4 Tbps and lasted up to 4 days.**

The concurrent rise in duration and capacity was enabled by the growing reliance on botnets — networks of infected devices. In fact, over **38% of attacks used botnets in Q1 2023.**

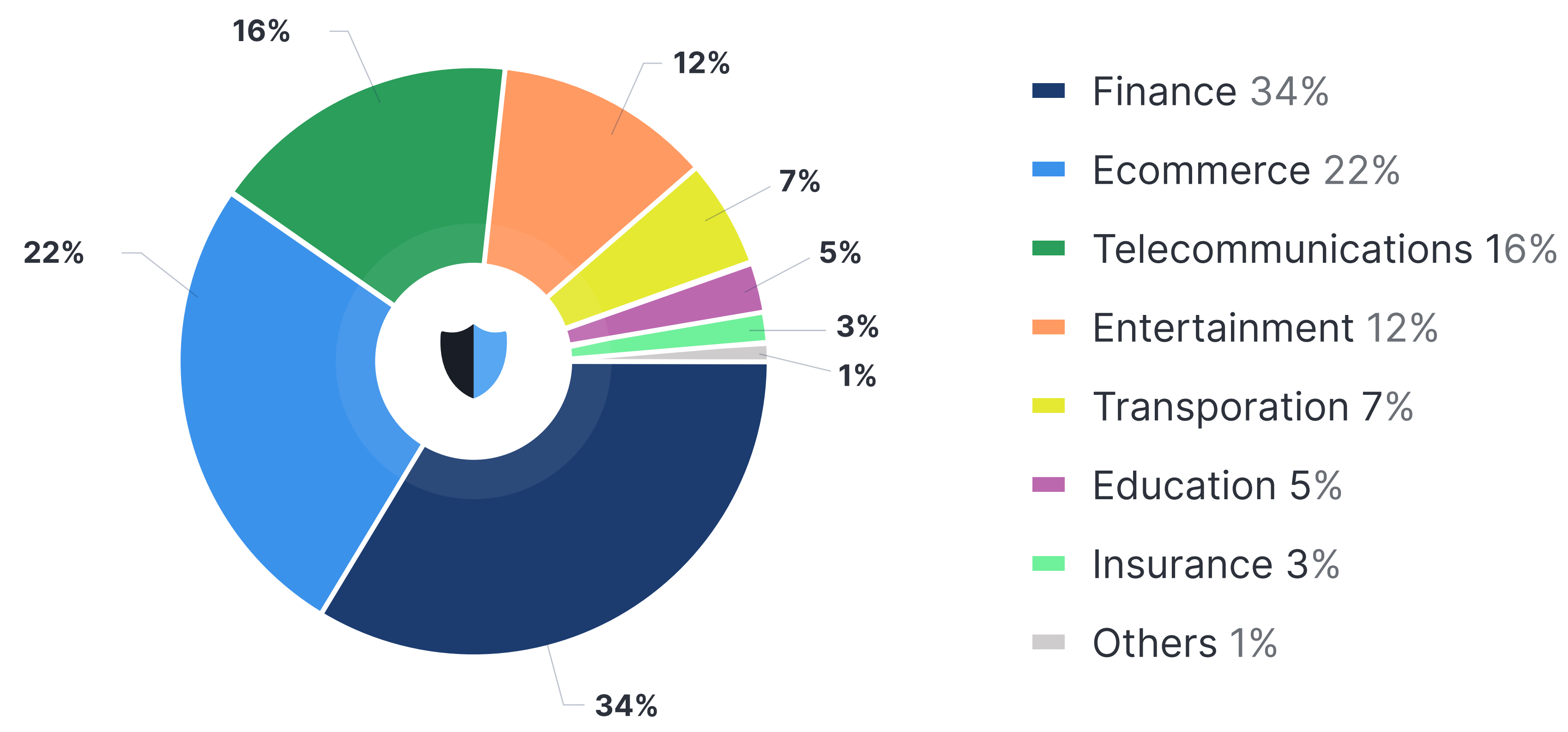
Q1 2023 DDoS Trends: an Overview

- Rise of smokescreening: DDoS attacks served as decoys in multi-vector assaults increased by 28% YoY. These assaults allow threat actors to distract security specialists while infiltrating networks or stealing data.
- Growing attack strength: The attack strength peaked at 1.4 Tbps, and the longest attack persisted for 4 days.
- Critical infrastructure targeted: To maximize damages, cybercriminals focused on overwhelming essential services like payment processors and logistical control centers.
- Botnets keep on gaining traction. Over 38% of DDoS attacks used networks of compromised devices.
- Decrease in political incidents: Hactivists were behind most DDoS attacks on Russian infrastructure in 2022; however, their activity significantly diminished in 2023.

Industry Breakdown: DDoS Attack Growth Rates Soar

DDoS attack frequency surged across most industries, reaching a new all-time high. Here's a year-over-year breakdown of the incidents breakdown by sector, from most to the least affected:

Shares of attacks by industry



1. Financial

In Q1 2023, the financial sector was the prime target, constituting 34% of attacks and witnessing a 68% YoY increase.

Predominantly, for-profit criminals attacked financial services' infrastructure, seeking to disrupt operations. Their objectives varied: from extortion and blackmail to diverting attention from data exfiltration, aiming to breach organizations and sell confidential information on the dark web.

2. Ecommerce

Ecommerce faced significant challenges, enduring 22% of attacks and a 51% increase compared to Q1 2022.

Q1 2023 saw a diversification in attack targets: not just ecommerce websites, but also underlying services like logistical services, supply chains, warehouses, and equipment manufacturers. This shift contrasts with many previous attacks, particularly during holidays, which often involved rival companies seeking to hinder competitors and gain market share.

3. Telecommunications

Telecom remained a popular target, with 16% of attacks and a 47% YoY increase, which places this vertical as the third most attacked.

Telecom providers' uninterrupted availability is vital for increasingly digitized online businesses. A telecom outage impacts numerous organizations within the affected area, putting immense pressure on providers to thwart attacks. This vulnerability makes them prime targets for threat actors pursuing extortion and blackmail opportunities. Smokescreening was also prevalent, as hackers aimed to obtain confidential information held by telecommunication providers.

4. Entertainment

The entertainment industry faced significant challenges, with 12% of attacks and a 36% increase in Q1 2023.

Video streaming services and online game servers were heavily targeted in this sector. Companies without professional DDoS protection struggled, suffering extended outages and leaving many players unable to enjoy their favorite games.

Users migrated to competitors with better-protected infrastructure that withstood attacks. Consequently, affected companies faced financial and reputational losses, as well as diminished market share.

5. Transportation

The transportation industry experienced the steepest growth in DDoS attacks. Despite accounting for only 7% of attack volume, attacks soared by 118% compared to last year's same period.

Transport hubs like traffic control centers, airports, and transport companies were prime targets for threat actors. This trend is concerning. Like most services, transport control centers rely on internet connectivity for seamless operation of systems such as traffic lights, subway signaling, and train automation controls.

Malfunctioning systems can cause significant transport hub delays, resulting in damages worth hundreds of millions of dollars and posing a direct risk to public safety. Prioritizing DDoS protection for transport systems is crucial, especially as we anticipate a continued surge in attacks on this sector.

Education and insurance

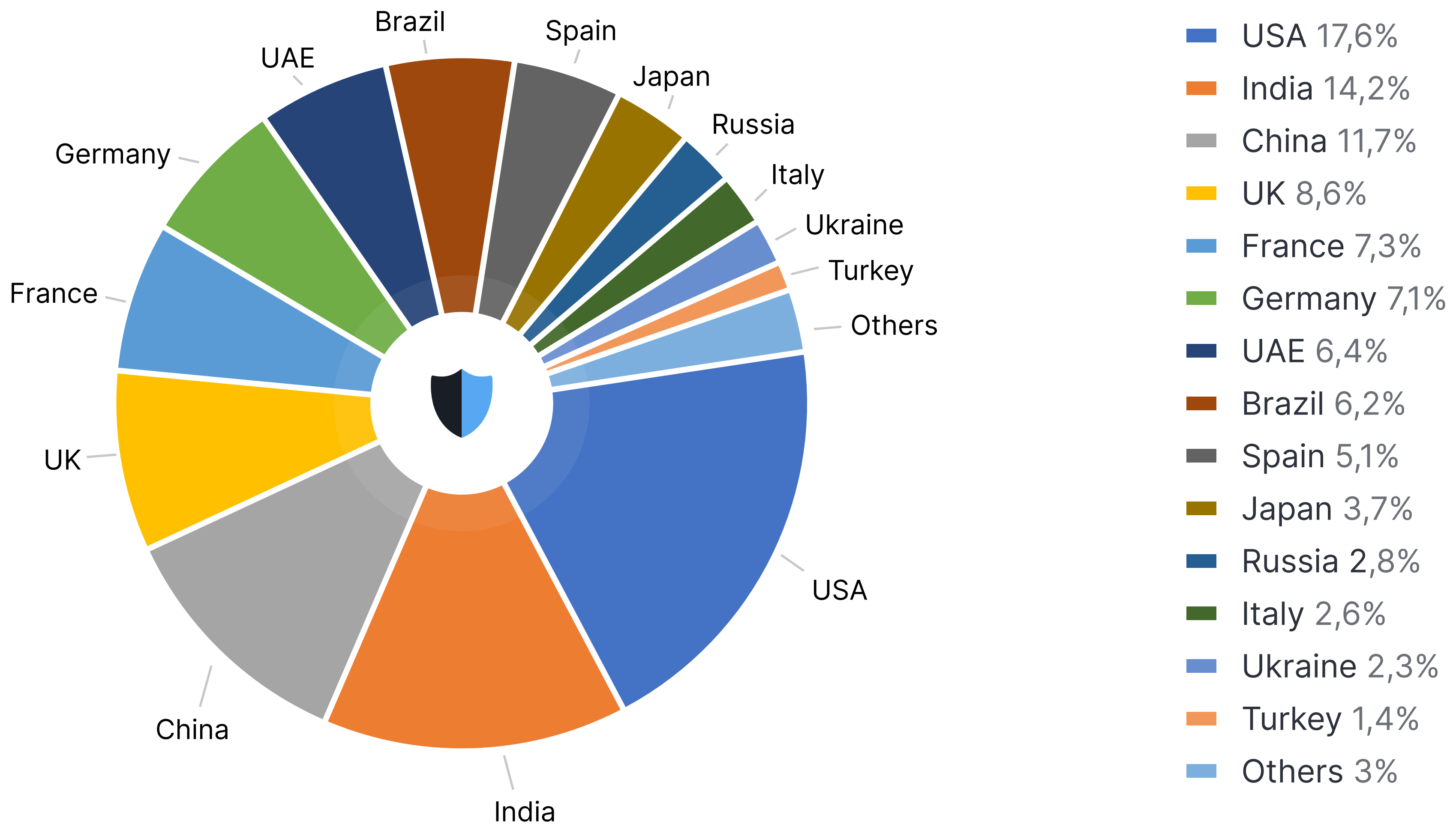
DDoS attack growth rates for education and insurance industries have stabilized, with attack shares of 5% and 3% respectively. Education incidents rose by 16%, while insurance saw a 5% increase.

Last year's surge in elearning attacks, partly driven by hacktivism, subsided in 2023. As lockdowns lifted and students returned to schools, attacks by students attempting to avoid exams also decreased. In the insurance sector, hackers primarily sought extortion and blackmail opportunities.

DDoS attacks breakdown by country

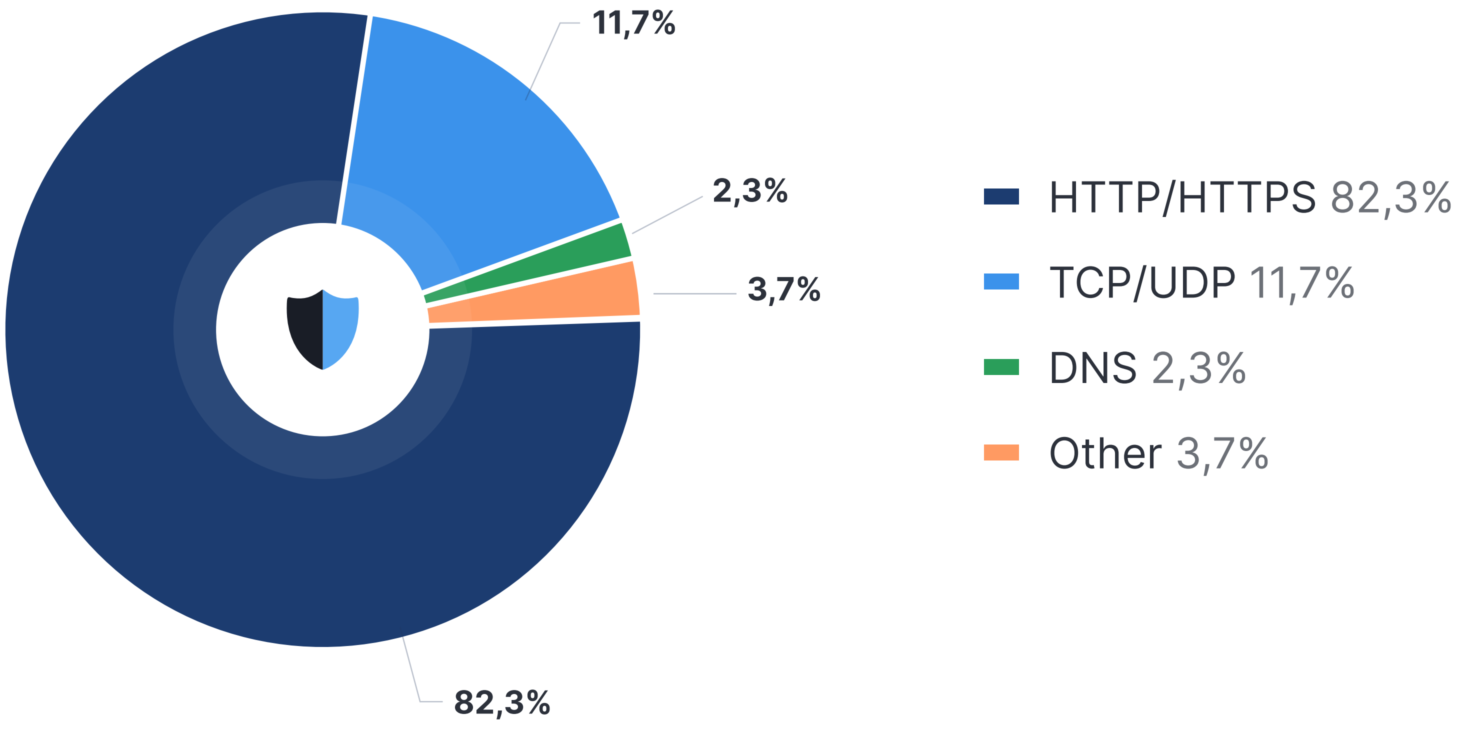
The United States, China, and India continue to top the list of the most targeted countries. A notable surge in attacks was observed in the United Arab Emirates, with their proportion nearly doubling from 3.8% in Q1 2022 to 6.4% in the current year. Conversely, both Russia and Ukraine experienced a decline in DDoS activity, resulting in lower rankings.

The following is a breakdown of countries by their share of DDoS attacks:



Protocol Breakdown

In Q1 2023, botnets are continuing to gain ground, causing the share of application layer attacks to balloon. On the other hand, transport layer attacks such as SYN floods or UDP floods have been on the decline.



Flood attacks targeting the lower levels of the OSI model tend to be less disruptive than those aimed at the application layer. While they can cause congestion and packet loss, these effects often do not render the resource entirely unresponsive. Consequently, as more damaging application layer attacks become increasingly accessible and cost-effective, the motivations for conducting TCP/UDP floods decrease, unless targeting a service specifically vulnerable to this type of attack.

Conclusion

Q1 2023 witnessed a near-universal rise in attack volume, strength, and duration, with emerging trends like the focus on transport hubs emphasizing the escalating threat of DDoS attacks.

Concerningly, threat actors have adapted their tactics, now integrating DDoS attacks within multi-vector incidents. This has forced targeted organizations to address not only outages from overburdened servers but also data breaches, ransomware, and additional threats. The emergence of these trends in merely the first quarter of the year is alarming and may indicate a potential escalation in the future.

In fact, based on data analysis from our client-targeted attacks, StormWall projects a 170% increase in DDoS attacks by the end of 2023. We recommend that all businesses seek professional DDoS protection to ensure their safety in the upcoming year.