2022: DDoS Year-in-Review Report by StormWall

StormWall's DDoS Year-in-Review report takes a look at the 2022 threat landscape, breaks down the industries that were most affected, and explores current DDoS trends.

DDoS attacks have evolved in 2022

Once more, 2022 became in many ways a record-breaker. As the criminals worked to build better botnets, multi-terabit per second attacks steadily increased in frequency.

While the maximum attack power hovered around 1 Terabit per second (Tbit/s) in 2021, this year it almost doubled: attacks reaching 2 Tbit/s became dangerously common in 2022.

Similarly, there was a steady increase in the duration of attacks throughout the year. By the end of 2021, most companies had to deal with incidents that lasted up to 3 days.

All this became possible thanks to the emergence of new sophisticated botnets. Originally developed by hacktivists for politically motivated actions, their use eventually spilled over to common criminals.

The beginning of the year was marked by a sharp spike in hacker and hacktivist DDoS activity in the first quarter. The trend carried over into the second quarter and then into the third. But the momentum blunted in the fourth quarter as hacktivist activity subsided.

Global DDoS attack trends in 2022

- Overall, there was a 74% YoY increase in the number of DDoS attacks in 2022.
- But the momentum took a turn in the fourth quarter. From the end of October, the growth rate began to slow down. The decline continued in November. And in December, the number of attacks plummeted by as much as 53% compared to the previous month.
- The year was marked by a dramatic increase in the power of botnets, which drove stronger and more sustained attacks.
- Criminals targeted the fintech industry more than others. It suffered 34% of the incidents. There's also been a 12-fold increase of attacks on financial services.
- Hacktivists contributed to the increase in the strength and duration of attacks, developing tools for politically motivated actions that were eventually adopted by for-profit criminals.

DDoS attack statistics by industry

Here’s which industries were most affected by DDoS:

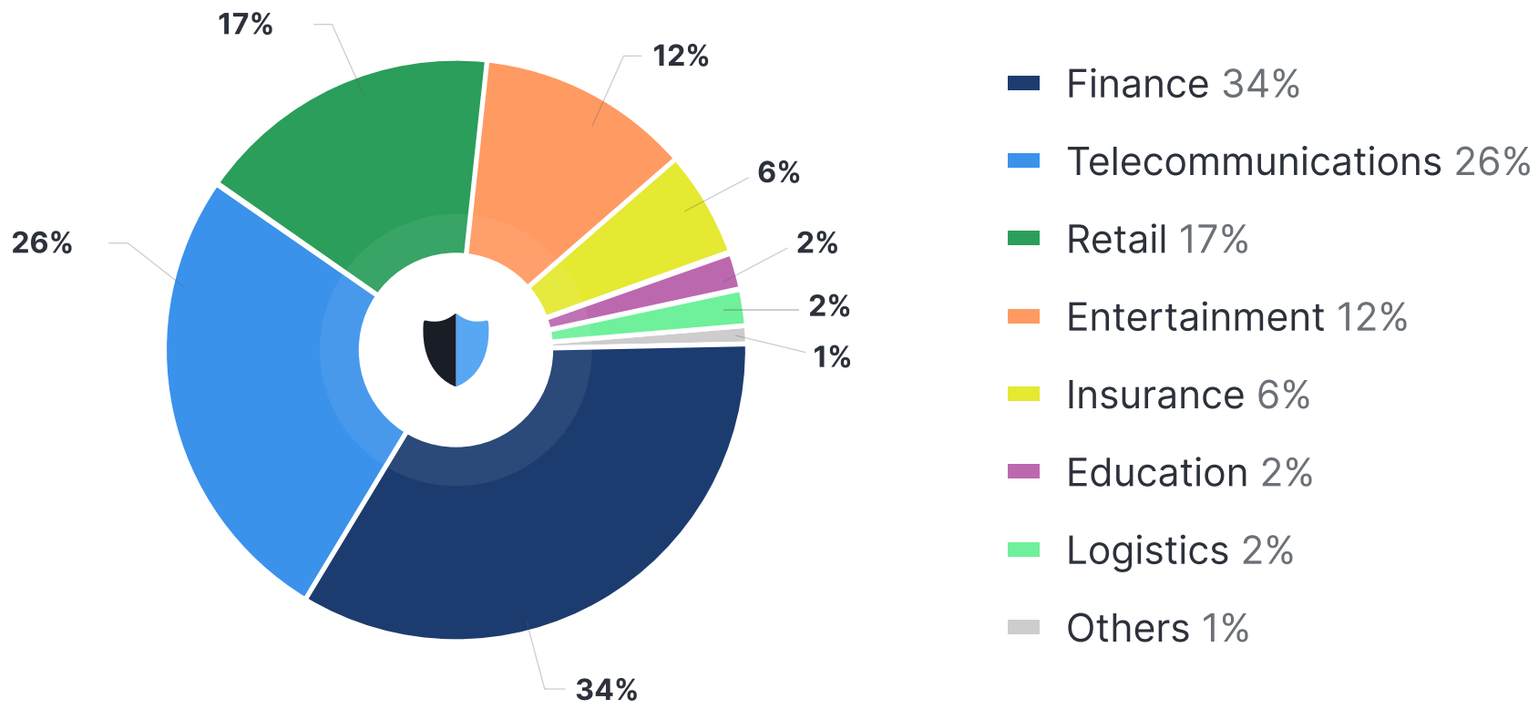

Figure 1. DDoS attack statistics by industry in 2022. Source: StormWall

Finance

In 2022, the main DDoS blow fell on the financial industry, with almost a third of all attacks (34%) targeting this vertical.

This sector also saw the sharpest growth, with attacks up 12 times year-over-year.

The fintech industry has traditionally been a DDoS hotspot. Threat actors often conduct powerful attacks on online financial services in an effort to disrupt payment processing. This is done as an extortion tactic or as a smokescreen to cover up a simultaneous malware or ransomware hack. But in 2022, a lot of incidents were initiated by hacktivists, especially in the first two quarters of the year. Though, their activity blunted towards the fourth quarter.

Attacks lasted an average of 8 hours, and the maximum power seen by StormWall reached 1 million requests per second. Such attacks are only possible using sophisticated botnets. This is one instance when tools, originally designed by hacktivists for their own use, are now beginning to see wider adoption, shaping the overall threat landscape.

Telecommunications

The telecommunications industry became a close-second in terms of attack numbers (26%). Attacks increased by 4 fold YoY.

As the pandemic forced many companies into remote working, video-conferencing became an indispensable driver of mission-critical business processes. Both politically motivated actors and for-profit hackers recognized the opportunity and began targeting businesses in this sector heavily. Attack goals ranged from hacktivism to extortion.

The peak attack power here reached 1,2 Tbit/s. The average duration was 8 hours. Many telecommunications companies have never faced a DDoS threat of this magnitude before.

Unprepared, the attacks disrupted their services slightly, but most companies remained relatively unscathed, avoiding major outages.

Most attacks on the industry can be attributed to companies trying to bring down the competition using DDoS. Also, hacktivists, who are constantly looking for new targets, began to hit businesses in this vertical.

Retail

The e-commerce industry accounted for 17% of DDoS attacks in 2022.

And there was a 53% YoY increase in the number of attacks on online stores. Most incidents were driven by unfair competition: companies launching attacks on peers to shut down competing stores and increase their market share.

As usual, the attacks peaked during the holidays, when shoppers rushed to online stores for gifts and discounts. There was a sharp spike in February the week before Valentine's Day (up 38% from the previous week) and in November, particularly around Black Friday and Cyber Monday.

The trend towards increased use of botnets continues here, as some of the attacks have been uncommonly powerful. And the average duration of attacks hovered around 3 hours.

This data paints a worrying picture. While e-commerce store owners had historically used DDoS for unfair competition, they didn’t usually employ botnets. These tools required a certain technical know-how, and were expensive to run. But this is all changing now, as botnet attacks are getting easier to launch and cheaper to maintain over long hauls. Thus, it is likely that such attacks will not only continue into 2023, but will also grow in destructive power and duration.

Entertainment

The entertainment industry suffered 12% of all DDoS attacks in 2022.

And the number of incidents increased 3 fold YoY.

As quarantine measures are being lifted across countries, users spend less time consuming online content. This somewhat downplays the ability of hackers to use downtime as leverage for extortion. Because of this, the share of attacks on the entertainment industry decreased by 12% from the previous year, and bad actors have shifted their attention onto other industries.

But the overall number of attacks is growing across all industries, which explains the 5-fold increase in the total number of incidents.

Insurance

Around 6% of DDoS attacks in 2022 targeted businesses in the insurance sector, constituting a 5 fold YoY increase.

Adversaries often seek opportunities to extort money from insurance companies. Likewise, business competitors may use malicious methods to gain a foothold in the market. DDoS attacks are particularly devastating for firms in this sector — they can incur substantial financial losses, customer attrition, and serious damage to the company's reputation. After all, an assured level of service availability is paramount for insurers.

Education

In 2022, the education industry accounted for 2% of DDoS attacks. Their number increased by 36% compared to the previous year.

Reliance on online learning has been growing rapidly since the pandemic. In fact, about 77% of public college students are now taking at least one course online. But the networks that accommodate this aren't sufficiently hardened. And DDoS attacks are so easy to launch now, that even students can do it. Indeed, some of the attacks recorded this year were launched by students who targeted their academy networks during exams.

But many incidents were also driven by hacktivists trying to disrupt college admissions campaigns in Russia: the first quarter of 2022 saw a sharp surge in attacks targeting the country’s universities.

Several websites that lacked professional DDoS protection experienced a prolonged outage. Many critical services were shut down, making it impossible for students to apply for admission. Such academies had to frantically connect DDoS protection to restore networks to working order.

Logistics

The logistics vertical accounted for a 2% share of DDoS attacks in 2022. And a 64% YoY increase in attack frequency was observed.

Digital enterprise supply chains rely on interconnected components: like links in a chain. Many are maintained by outside vendors, and the client essentially has to trust in their ability to secure these systems. But some vendors still use open source software, and some have relaxed their security measures in the post-pandemic world of remote work. This creates a huge vulnerability and leaves otherwise resilient companies vulnerable to attacks.

Supply chains are only as strong as their weakest link, so shattering one can bring the whole thing down. Of course, hackers quickly seized the opportunity, distracting cybersecurity teams with DDoS while staging backdoor attacks. This can result in breaches and leaks of confidential data.

But for-profit criminals weren’t the only source of danger this year. Hacktivists also launched a series of large-scale DDoS offensives against logistics businesses in Russia, in an attempt to disable critical supply chains.

DDoS attacks by protocols

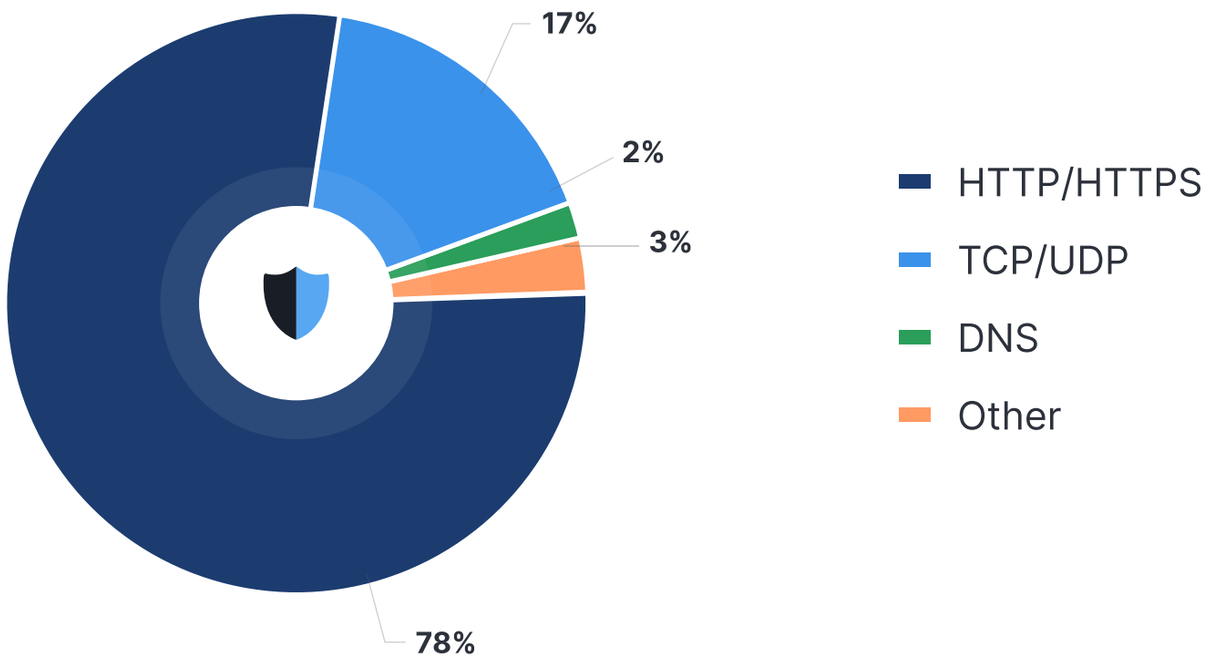

Figure 2. Dynamics of protocol attacks in 2022. Source: StormWall

The vast majority of DDoS attacks in 2022 (78%) were directed at the application layer of the OSI model.

Only 17% of attacks hit the network and transport layers, and even fewer attack the DNS (3%).

Interestingly, the distribution of attacks by protocol is reversed compared to last year. In the third quarter of 2021, more than 80% of attacks were packet flooding, targeting the transport and application layers. Maintaining HTTP floods capable of constantly overloading enterprise networks was simply too expensive. This year, everything has changed, as the cost of using sophisticated botnets has decreased while their firepower, on the contrary, has increased manifold.

This has forced businesses into a race to rethink DDoS protection, as the security measures implemented to increase their resilience against TCP/UDP floods are now insufficient.

DDoS attacks by country

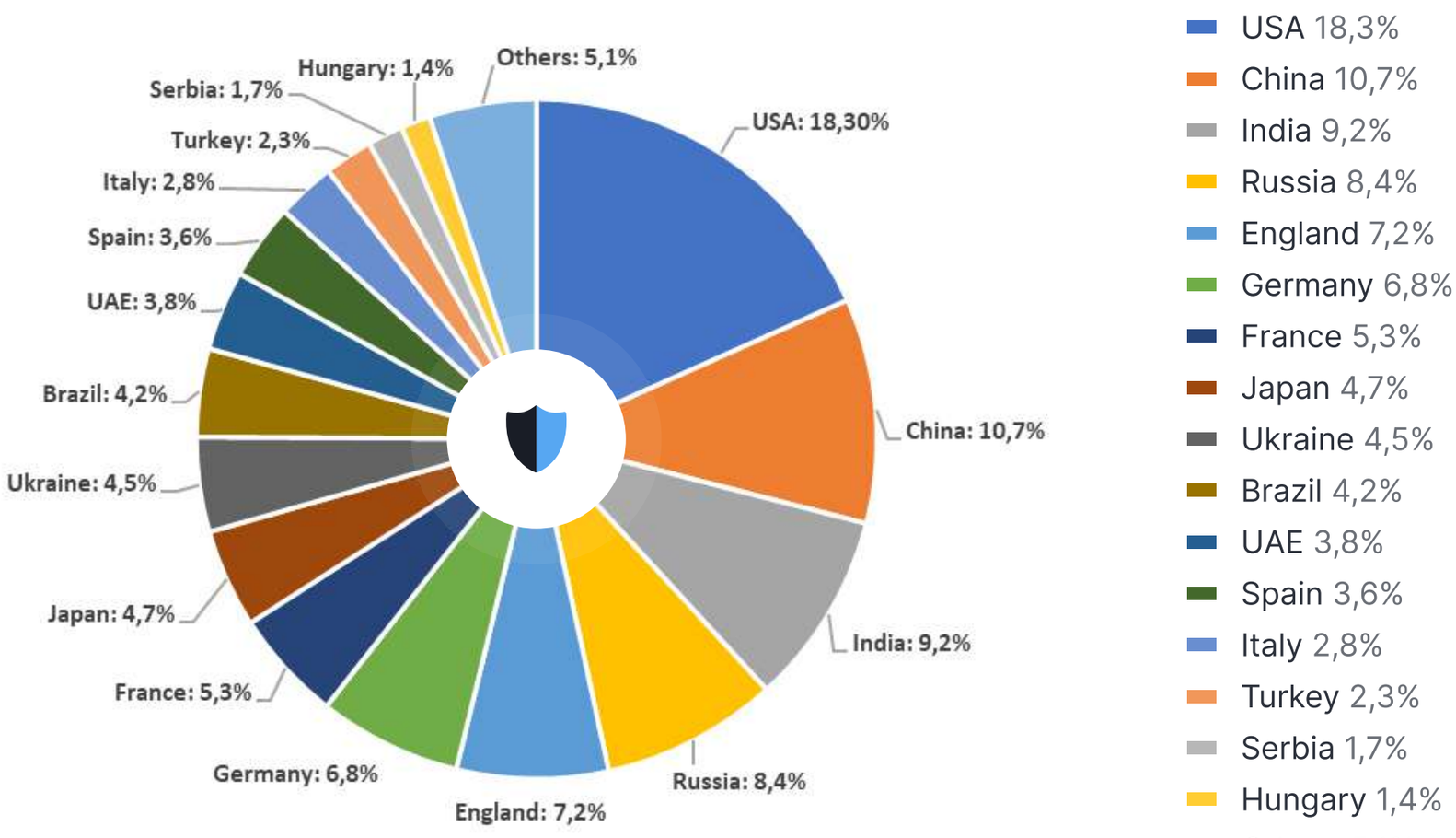

Figure 3. DDoS attack statistics by country in 2022. Source: StormWall

The US was struck by 18.3% of all DDoS attacks, bearing the heaviest blow. Like elsewhere in the world, the number of attacks peaked in the first and second quarters of the year. The trend then began reversing in the third quarter, and flipped downwards in the fourth. Threat actors were most active on Fridays, potentially hoping to catch security teams unawares at the week's end.

China, which was hit by 10,7% of attacks, was the second hottest DDoS hotspot this year. China is traditionally a major source of global DDoS traffic.

India was a close runner up for the undesirable 2nd place. It came in third, with 9.2% of incidents finding their targets in the republic. Some attacks can be attributed to hacktivism, but it wasn't the only driver. Some incidents were carried out for the purpose of extortion, or as part of multi-vector hacks.

Russia, the fourth most attacked region, got hit by 8,4% of DDoS attacks. Obviously, this is due to the Russia — Ukraine conflict, which understandably made the former the main target of hacktivism. All industries were affected, from education to finance, as independent and state-sponsored gangs put the country under a real barrage. They tried hard to cripple critical infrastructure, paralyze businesses and banking, and sabotage the economy as a whole.

A more trivial story took place in **the UK**, where 7,2% of DDoS attacks landed. As one of the most developed economies in the world, it is typically targeted by for-profit criminals, who are trying to hit the jackpot.

Conclusion

This year, DDoS actors have advanced and pretty much doubled their firepower. Unfortunately, the same cannot be said for most organizations, whose resilience to DDoS is dwindling as attack duration and power grows faster than businesses get better at mitigation.

And the impact of these attacks cannot be overestimated. If successful, they can cause days of downtime, disrupt learning, restrict access to information, and even banking. The threat will only grow. That is why StormWall recommends all companies to work with a professional security partner to build up their DDoS resistance.