Q2 2023 in Review: DDoS Attacks Report by StormWall

StormWall, a global DDoS protection provider, has studied Q1 2023 attacks on their clients across various sectors: financial, e-commerce, telecom, entertainment, transportation, education, and logistics, for their Q2 2023 report.

Global DDoS Trends in Q2 2023, an Overview

Q1 2023 marked a significant rise in attacks, sustaining the growth trajectory from the previous quarter with a **68% Year-over-Year (YoY) increase in DDoS attacks**. At the same time, StormWall experts noticed a clear move towards an increased usage of botnets.

This manifested in spiked activity of known threats, such as the Mirai botnet, but new and concerning malware types have also emerged. For example, Condi botnet specifically targets certain router models from TP-Link, and HinataBot, an offshoot of Mirai, started operations at the beginning of the year but managed to elude detection by security researchers for a considerable period.

This trend goes hand in hand with the growing number of devices connected to the Internet, or the "Internet of Things" (IoT), which gives more room for botnets to grow.

Cybercriminals mainly targeted finance (26% attack share), telecom (17% share) and entertainment (14% share) verticals to cause disruption and damage core national economic pillars.

These targets are usually well-protected with website protection, server protection (TCP/UDP), network protection (BGP), or a combination of multiple services. The fact that adversaries successfully target such companies means the attacks are getting increasingly more sophisticated.

In Q2 2023, multi-vector attacks saw a massive 136% increase compared to Q2 2022. These attacks strike at multiple network layers and elements within an organization's infrastructure. Hackers concurrently target a company's site, network, and infrastructure to inflict maximum damage. Not only are such attacks potentially incredibly destructive, but they can be difficult to recover from.

We also saw more attacks on government organizations, healthcare systems, and transportation services. This shows a shift towards targeting essential services, which could severely affect a lot of people.

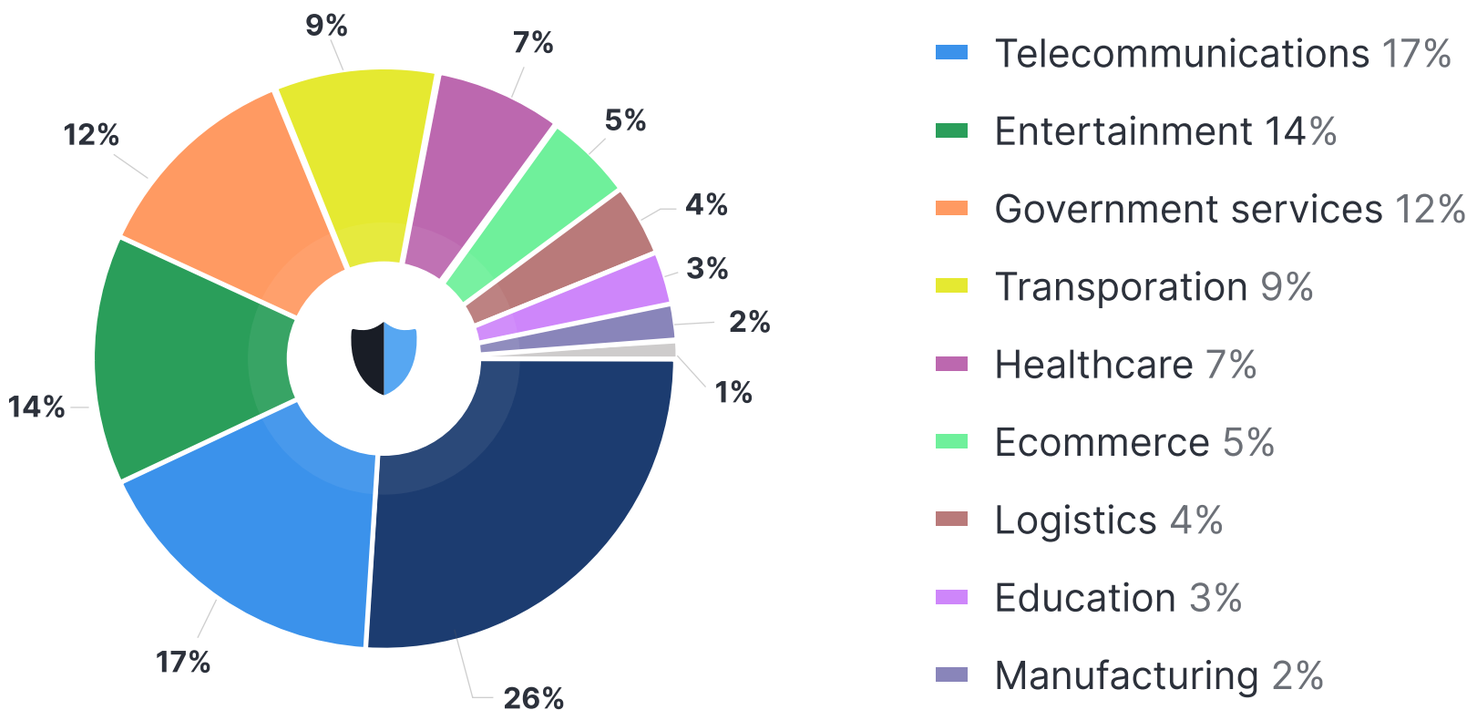
Q2 2023 DDoS Trends: an Overview

Here’s a look at the trends that dominated the DDoS landscape in the second quarter of 2023:

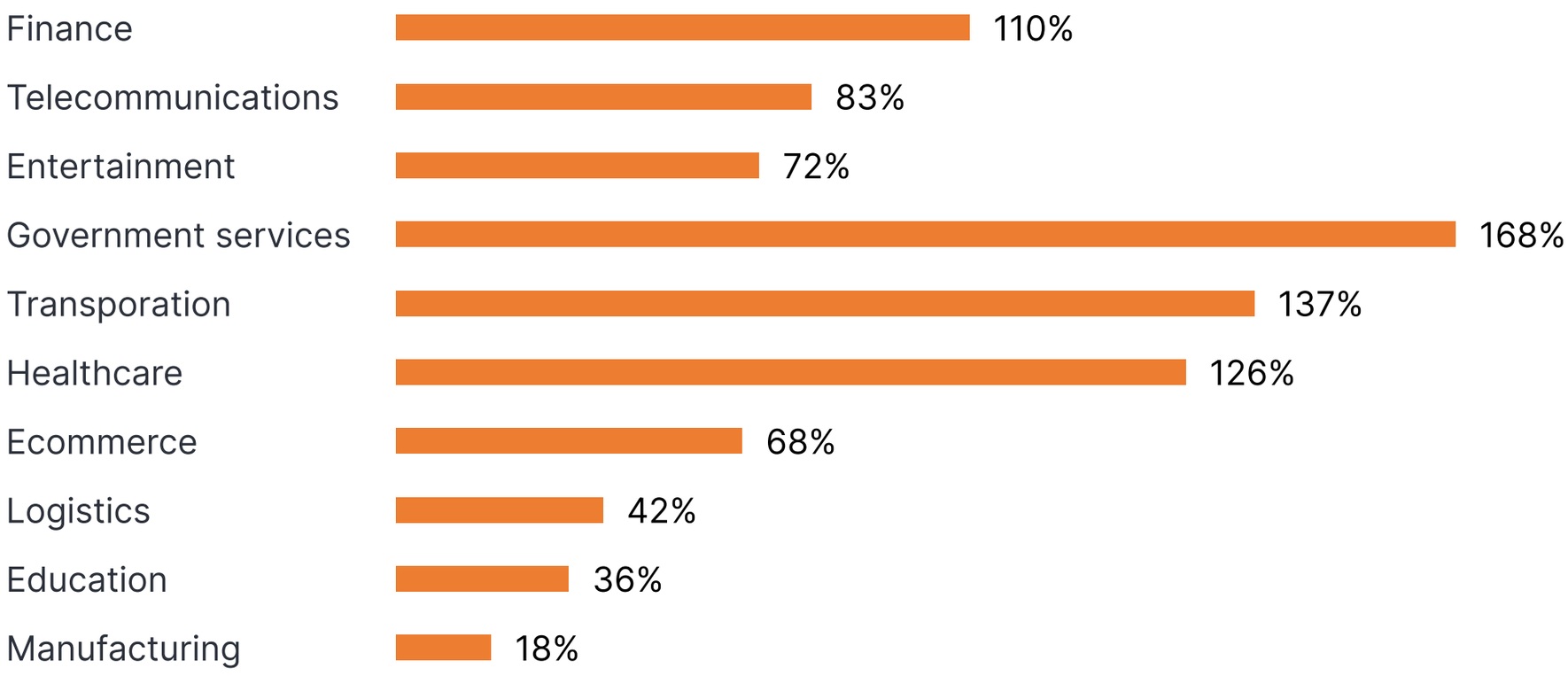
- **Rising tide of botnet usage**: the increasing reliance on botnets for attacks coincides with the continued expansion of the IoT.
- **Multi-vector attacks up 136%**: hackers target multiple network layers simultaneously to inflict maximum damage. Such attacks hit hard and are difficult to recover from.
- **Shift in target sectors**: cybercriminals have been targeting critical industries such as finance, entertainment, and telecom, while increasing their attention on government, healthcare, and transportation systems.
- **IoT and Growing Botnets**: as more devices join the Internet of Things (IoT), botnets continue to expand. This enables threat actors to carry out more powerful attacks. Some of these botnets are made up of Virtual Private Servers (VPS) rather than Internet of Things (IoT) devices. These variants are highly-performant and capable of launching hyper-volumetric attacks.
- **Emphasis on essential services**: to maximize disruption, the focus has been redirected towards crucial systems and services, causing significant concerns for sectors such as government, healthcare, and transport.

Industry Breakdowns: a Record-Breaking Quarter

Shares of attacks by industry



Increase in attacks compared to Q2 2022



1. Finance

In Q2 2023, the financial sector tops the list as the most targeted vertical — it sustained 26% of attacks and saw a 110% YoY increase, which is nearly double compared to the last quarter this year.

Many of these incidents were politically motivated, the recent attack on the European Investment Bank (EIB) being a case in point. This particular assault disrupted various web services of the EIB, underlining that without proper safeguards, financial infrastructures remain susceptible to DDoS attacks.

Heightening political tensions within Europe fuel a conducive environment for hacktivism.Threat actors with political aims often target important sectors, such as finance and government services, to create the most disruption possible. We can expect to see more such attacks in the future.

2. Telecommunications

Telecom vertical accounted for 17% of attacks and experienced an 83% YoY increase, making it the second most attacked industry in Q2 2023 (up from the third spot last quarter).

The rise in attacks can be linked to the spread of IoT devices which are often used to drive botnet attacks. Once mostly concentrated in conflict-stricken parts of Europe, these attacks have now expanded globally, posing a risk to critical infrastructure and services beyond just telecom networks.

These attacks are usually carried out by bots — a type of malware that searches for weak devices — a strategy connected with several IoT botnets. With billions of IoT devices around the world, ranging from smart fridges to smartwatches, and many having poor security, cybercriminals have a wealth of targets to exploit.

Hacktivism played a role in some of these attacks, like the recent incident impacting various telecom and financial services in Israel. Extortion and smokescreening also emerged as key objectives in these cyber assaults.

3. Entertainment

The entertainment sector faced 14% of total attacks, marking a 72% year-on-year increase.

Video streaming platforms and gaming servers were prime targets for cybercriminals, leading to significant disruptions for users. It's likely these attacks were motivated by extortion and financial gain. Notably, the launch of Diablo 4, a much-anticipated action role-playing dungeon crawler from Blizzard, was impacted as servers buckled under an attack, causing widespread disappointment among gamers.

Servers for multiplayer shooters Call of Duty and Overwatch were also affected in unrelated incidents. Servers of multiplayer games are particularly vulnerable to DDoS attacks as any delays can severely impact the gaming experience.

4. Government services

In a new category for this quarter's report, government services accounted for 12% of the attacks. This sector saw a staggering 168% year-on-year increase in attacks, marking a record-breaking surge.

A majority of these incidents were instigated by politically motivated and state-sponsored threat actors, carrying out campaigns at a scale not seen in several months. Government agencies in Russia, Poland, Switzerland, Germany, and the US were affected, among others. Russian institutions in particular were heavily targeted, seeing a 74% increase in attacks in May compared to the same period last year. This happened as political tensions continued to escalate.

As of the time of writing, there's no indication of these attacks slowing down. Many incidents reached beyond government sites, hitting transport hubs and healthcare facilities.

5. Transportation

Attacks on airports and railway hubs are on the rise, with the transportation sector now accounting for 9% of incidents and seeing a massive 137% year-on-year increase. This makes it the second fastest-growing vertical, following closely behind government services.

This is happening amid calls for increased security. Transportation services rely on a vast network of interconnected systems. Under the right conditions, an attack on these hubs can do more than cause, it can trigger an incident.

However, key transportation hubs are essential economic assets, a fact that hasn't gone unnoticed by hacktivists. Recently, politically motivated attacks have sought to disrupt these transport hubs, aiming to derail state visits and cause broader disruption.

6. Healthcare

In **healthcare**, we've recorded 7% of attacks and a 126% YoY increase.

This is closely tied to the rapidly increasing attack on government services, which often spill over into other critical infrastructure. Nonetheless, healthcare providers should exhibit caution: they're in the third fastest growing vertical in terms of DDoS attacks.

While some attacks are politically motivated, others aim for financial profit. DDoS attacks can hinder essential healthcare services, blocking doctors from accessing patient records, causing equipment malfunctions, and even disrupting ambulance routing. This can prevent patients from receiving urgent care. Knowing the time-sensitive nature of healthcare, hackers leverage this urgency in their extortion attempts.

7. Ecommerce

The **ecommerce** industry made up 5% of the attacks and experienced a 68% growth.

This aligns with the trend we've been observing for several months. The majority of these attacks pursued extortion, or were carried out by rival ecommerce businesses seeking to knock out competing sites and increase their own market share while the competitors were down.

Extended outages can lead to substantial financial losses for retailers, as they prevent customers from completing online purchases.

8. Logistics and Education

The **logistics** and **education** industries accounted for 4% and 3% of the attacks respectively, with year-on-year growth rates of 42% and 36%. In the logistics sector, the goal was often to disrupt supply chains, with attacks driven by both hacktivism and profit motives. Meanwhile, incidents within the education sector were largely attempts to disrupt exams in schools and higher education institutions.

9. Manufacturing

While the manufacturing sector only accounted for 2% of attacks, it's a new and worrisome addition to our list, experiencing an 18% year-on-year increase. Attacks on manufacturing plants can critically damage industrial control systems (ICS), leading to control failures and severe economic repercussions for the affected companies. Many manufacturing facilities depend on IoT devices, which are frequently targeted by malware to form botnets.

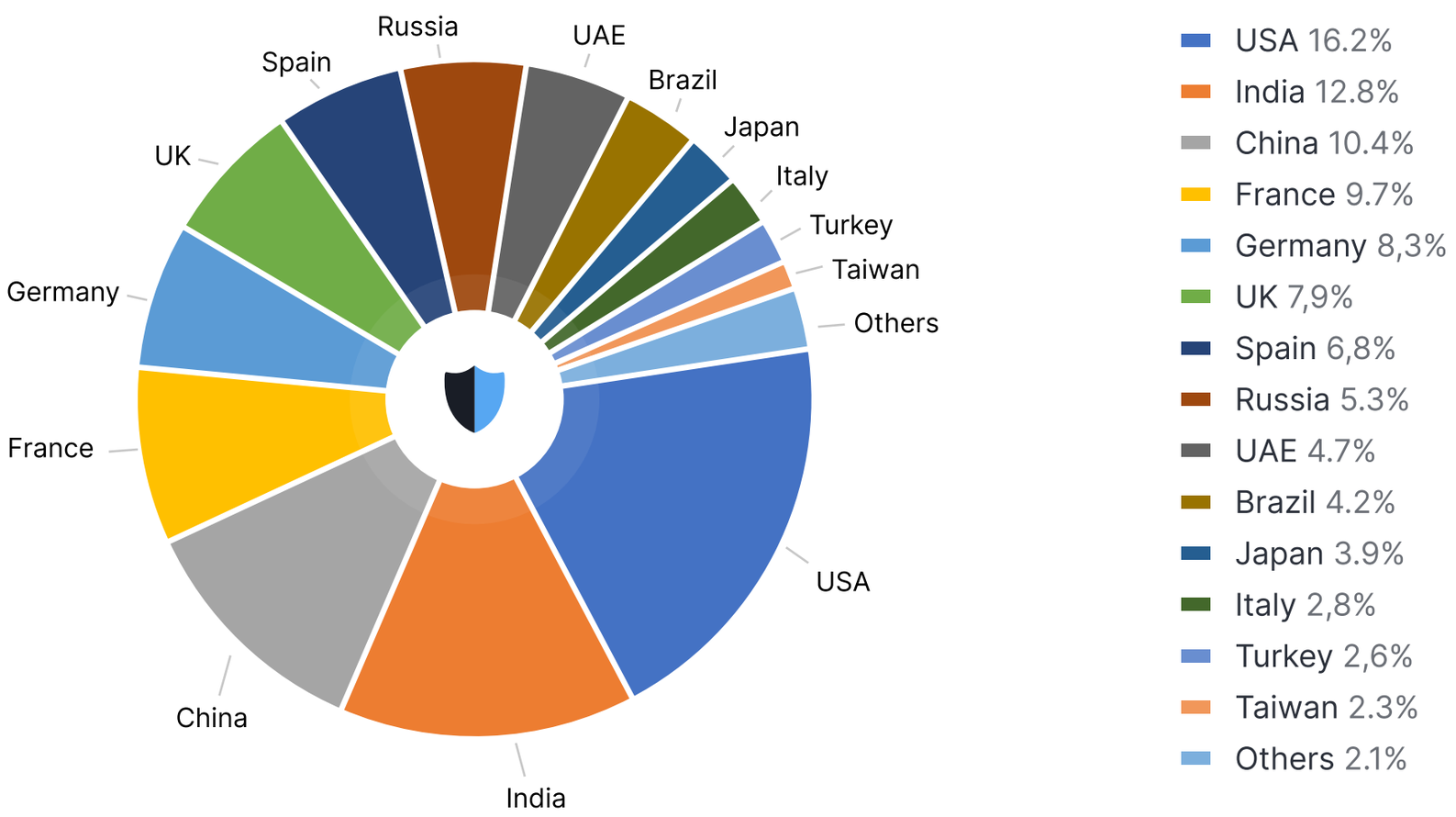
DDoS attacks breakdown by country

The United States, India, and China continue to occupy the top spots as the most targeted nations for DDoS attacks. Compared to Q1 of 2023, The US saw a slight decrease in the percentage of attacks, going down from 17.6% to 16.2%. India also experienced a minor decrease, moving from 14.2% to 12.8%.

The most significant change can be observed in France, which saw its share of attacks rise from 7.3% to 9.7%, becoming the fourth most targeted country.

Germany's share increased from 7.1% to 8.3%. The UK faced a slight decrease, from 8.6% to 7.9%. Spain saw an increase, moving from 5.1% to 6.8%. In contrast, Russia also experienced an increase from 2.8% to 5.3%. While the UAE's share decreased slightly from 6.4% to 4.7%. Brazil's share decreased from 6.2% to 4.2%. Japan, Italy, and Turkey all saw slight decreases.

Here is the distribution of countries based on their share of DDoS attacks this quarter:



Conclusion

Q1 2023 recorded an unprecedented growth in DDoS attacks across key industries. Notably, government services saw the highest rise at 168%, closely followed by the transportation sector at 137% and healthcare at 126%.

This significant increase, made possible in part by the emergence of new botnets, indicates an escalating cyber threat landscape. Worryingly, sectors which are historically heavily attacked such as finance and telecommunications have also experienced a notable increase of 110% and 83% respectively.

Alarmingly, there's a rapid shift towards more disruptive techniques, like multi-vector DDoS attacks. These campaigns, hitting various layers of an organization's infrastructure all at once, surged by 136% YoY.

All this has been fueled by a rise in botnet usage. This trend heightens the risks for organizations lacking DDoS protection, making them prone to severe and extended outages.