MAZEBOLT

DDoS Attack Summary 2022

REPORT

2022 is coming to an end, and it was an eventful year. 2022 saw worldwide elections, from the US mid-term to governmental elections across Europe. The war between Russia and Ukraine continued. Many countries continued adjusting to new procedures and social trends following the global pandemic of 2020. The entertainment and gaming industries are adjusting products to new consumer behavior, and the global economy still tries to find a welcomed balance. In the midst, airlines and the entire travel industry are still evolving their methods and practices to the new social conformities, and we even had the soccer World Cup. And the one thing that connects all these changes and adjustments is the rising number of DDoS attacks.

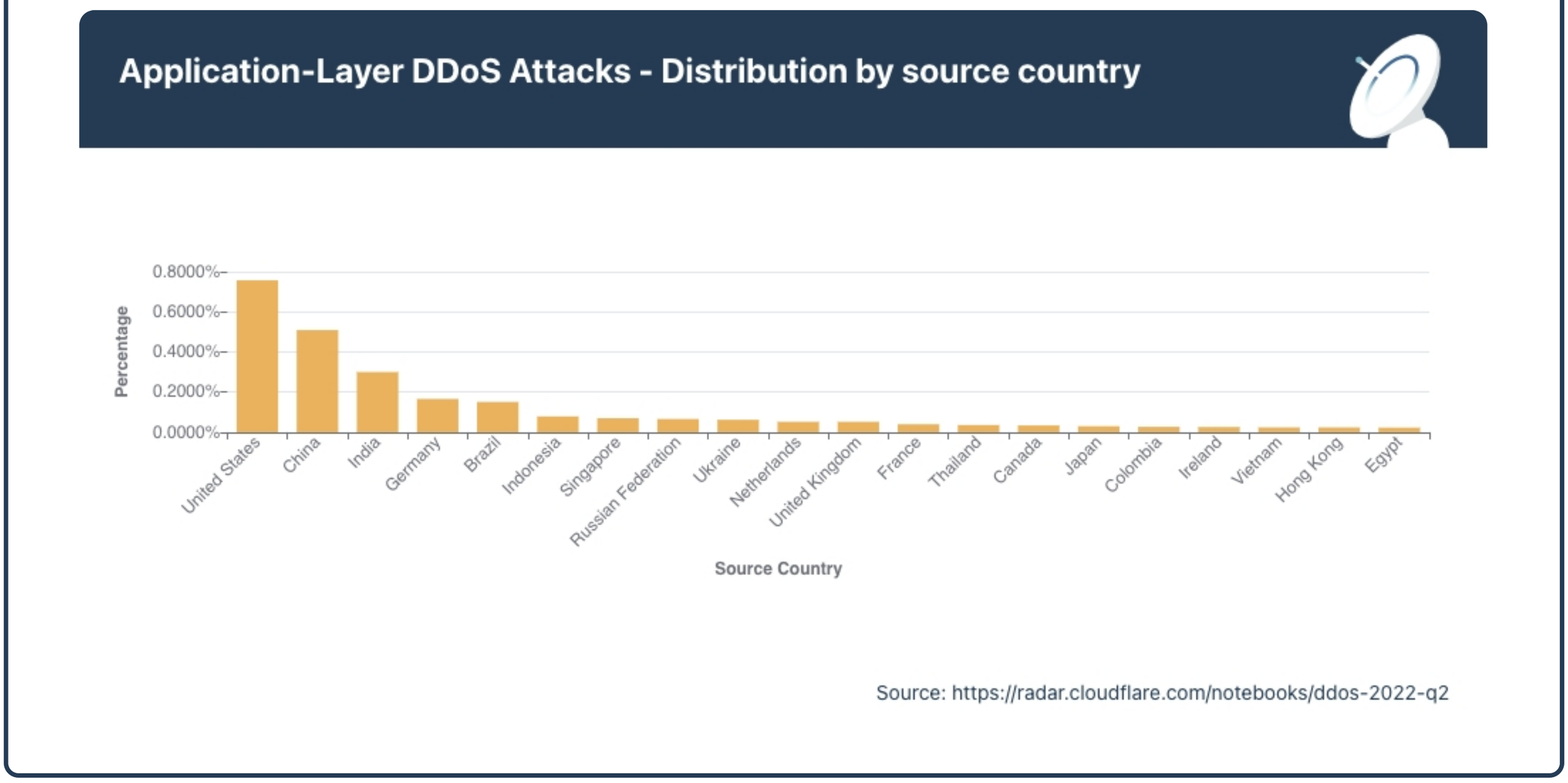
As networks become more complex, DDoS attacks have become more sophisticated and malicious, and are the current leading cyber threat in the world. DDoS attacks have become more frequent and damaging to organizations around the world, and 2022 saw DDoS attacks turning into a major global cyber threat. Due to their relatively simple execution, DDoS attacks have become the weapon of choice for threat actors worldwide. They seek to disrupt organizations' activity, sometimes even perform ransom attacks.

In 2022, governments and financial organizations from various fields continued to be the most sought-after targets for DDoS attacks, with these attacks spanning and reaching every major country and field of operations. In addition to governments and financial institutions, 2022 saw a worrying rise in gaming companies being attacked by DDoS. In this report, we will sum up the leading 2022 trends in DDoS attacks. DDoS attacks are not going anywhere in 2023. On the contrary, the rising number of successful DDoS attacks indicates that this cyber threat will only continue to evolve. We encourage organizations to embrace change and take a more proactive approach to protect their dynamic attack surface and strengthen their DDoS resilience.

Some numbers, to begin with

According to several studies and reports, the average successful DDoS attack in 2022 lasted for over 50 hours, compared to 2021, where the average was 30 minutes. This, of course, indicates that DDoS attacks are evolving to become more sophisticated and malicious. The month of June saw a record-breaking DDoS attack on Google's Cloud Armor, with 46 million requests per second, launched from more than 5,000 IP addresses originating from over 130 countries. Almost 30% of this attack traffic originated from Brazil, India, Russia, and Indonesia. Reports indicate that there was a 67% rise in Ransom DDoS attacks in 2022, compared to 2021, and that most attacks begin on Fridays, close to the end of the business week – when most organizations are understaffed.

Reports indicate that most DDoS attacks during 2022 were targeting the US, with almost 44% of total attacks. China and Germany experienced 8% and 6% of reported attacks, respectively. It is also important to note that the US is also the main source of HTTP DDoS attacks, and that a high percentage of DDoS activity in a specific country doesn't mean that that country is launching the attacks, but rather that the presence of botnets operating from the county. A recent report by a leading research institute in the US showed that during a DDoS attack, every minute of downtime costs over 20,000 USD, while getting back online and remediating the damage caused by a DDoS attack averages in 120,000 USD. As in recent years, 2022 saw a rise in multi-vectored attacks, with over 60% of DDoS attacks classified as such. At the end of 2022, there are currently over 15 million active IP's that can be used to launch a DDoS attack, and the number keeps rising daily.



Who were the leading DDoS attacks targets in 2022?

Continuing the 2021 trend of attacking various governmental sites, 2022 saw a rising number of successful DDoS attacks on many governments and governmental services, Everyone, everywhere, is a target. The reasons behind these attacks vary from ideological, such as attacks against the Russian and Ukrainian governments or governments who show support in each side of this conflict, to disruptive, such as attacks against the Greek and Lithuanian governments. Some attacks were launched against governments who showed support with either side of the Russia/Ukraine war, such as the attack against several Eastern European governments, with an emphasis on their intelligence services - Poland, Romania, Bulgaria, Moldova, and Estonia. Similar attacks were launched against the Vatican and Belgium.

The US and UK governments were attacked as well, both during their elections, with the UK's MI5 also being attacked. This latest MI5 attack is similar to an attack that took place against the German government. That attack was a simple one, but it did shut down the Defense Ministry and the Federal Police's sites for several hours. The Israeli health

ministry was attacked in 2022 in an attempt to cause disruption, and so was the Italian government, which suffered an attack on various offices and important services, due to the Italian government's support of Ukraine.

Other countries that suffered severe DDoS attacks in 2022, with an emphasis on major disruption of crucial services and utilities, such as airports, healthcare and electrical were India, Japan, Taiwan, Lithuania, Sweden, Finland, Latvia, Indonesia, and North Korea. The latter literally disappeared from the internet for almost an entire weekend in the beginning of the year, with many conflicting reports as to who performed the attack and why. The North Korean government explained the incident as a power outage, but cyber experts worldwide confidently assume that the country was under a severe DDoS attack, possibly targeted by threat actors based in either China or the US.

Financial institutions are the runner-up

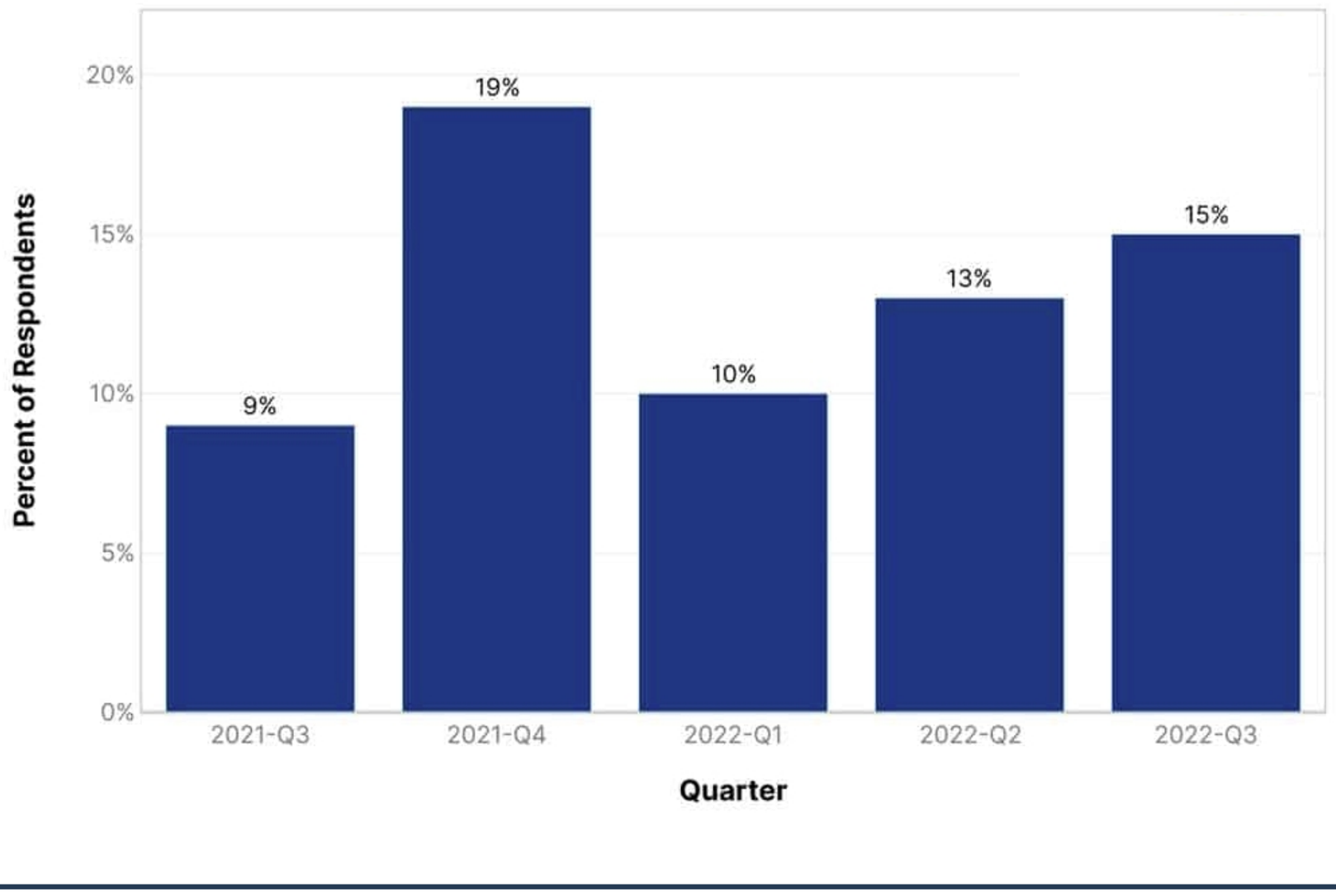
2022 saw a rising number of successful DDoS attacks targeted at financial institutions and organizations, from various fields. The leading type of organization to be attacked were banks, worldwide. Following banks, 2022 saw a worrying rise in attacks against trading companies and even some NFT organizations, such as "Swissqoute" from Switzerland, with its servers being the target of a severe DDoS attack in November. The beginning of the year saw another attack against an American Cryptocurrency organization that suffered four different attacks during 2021. Reports suggest that these attacks, which spilled into 2022, might be the cause of aggressive competition between blockchain platforms that may have led to these DDoS attacks, but there's no official confirmation of such theories. But one thing is for sure, and it's that the immediate damage following these DDoS attacks was significant downtime. Long term damages are yet to be disclosed, but one can assume that the attacked platform, Solna, lost many clients to its rivals.

There’s no doubt that financial institutions and banks suffered more DDoS attacks in 2022. In fact, just in the first two quarters of 2022, there has been a steep incline in DDoS attacks related to financial institutions. The UK’s FCA (Financial Conduct Authority) reported that 25% of cyberattacks reported were DDoS, compared to 4% in 2021. The UK’s FCA regulates the activity of more than 50,000 financial services firms. If any of these organizations experiences a cyber incident, they must notify the FCA immediately.

“We’re seeing a surge in DDoS attacks against financial institutions due to the acceleration of digitization in the industry,” comments Matthew Andriani, CEO of MazeBolt. “This growth is accompanied by an expanding, complex attack surface in which they have no visibility, leaving them extremely vulnerable to DDoS attacks. Financial institutions must use 2023 to gain critical insight into their DDoS attack surface in order to effectively mitigate, remediate, and ultimately reduce their DDoS risk.”

Ransom DDoS Attacks & Threats by Quarter

Source: Cloudflare

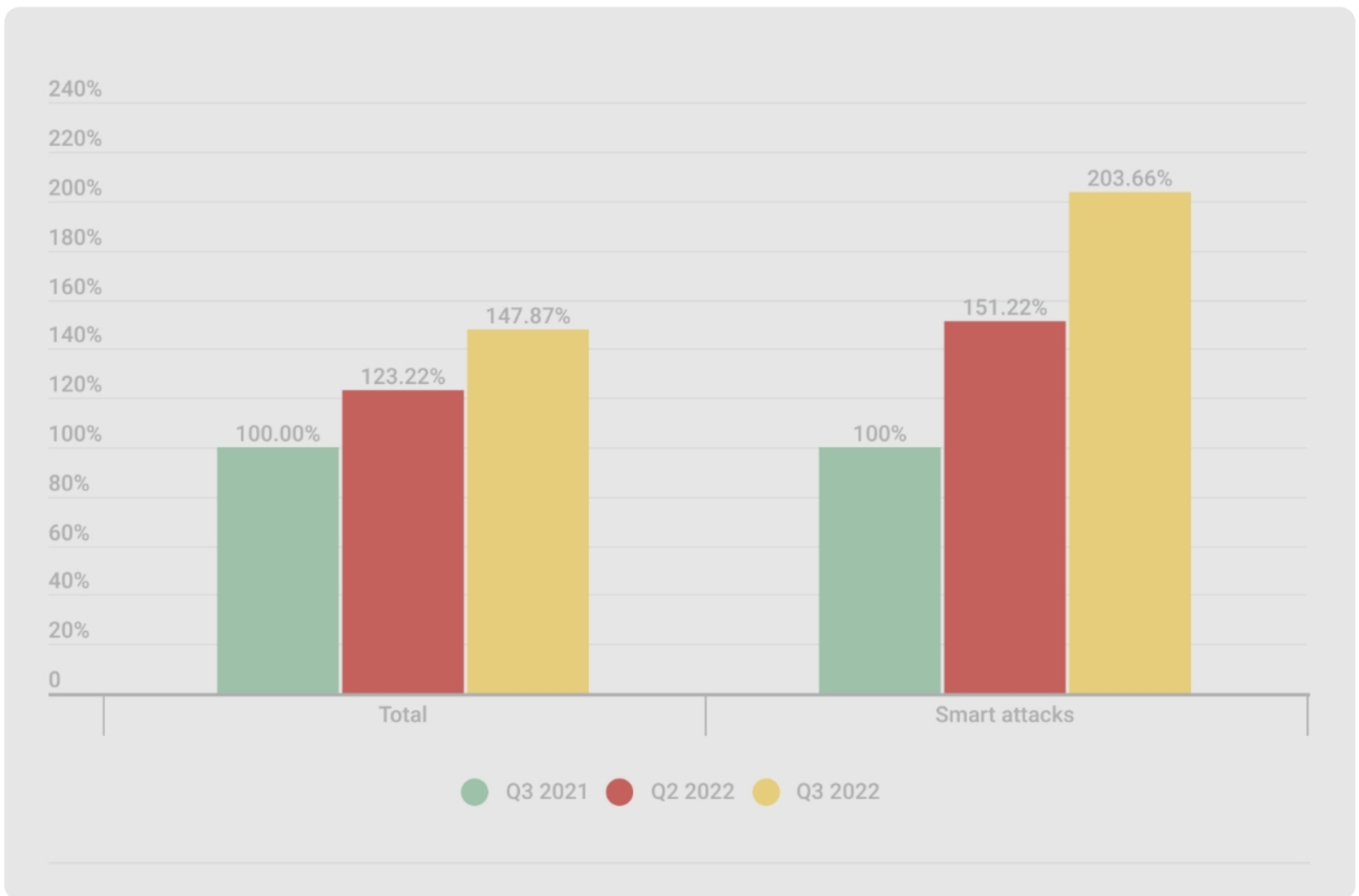


Gaming companies should start to worry

Over the past year several major gaming companies came under DDoS attacks, with some of them being targeted on multiple occasions. “Activision Blizzard” was attacked twice, with both attacks shutting down the company’s operations for several hours. “Final Fantasy” was attacked twice as well, while “Minecraft” was targeted in a large-scale attempt that was successfully blocked, but after causing major disruptions to the company’s operations, which was forced to allocate many resources to block the attack. “Andorra Telecom” was attacked during a large-scale multi-day Twitch gaming tournament, resulting in little to no internet connectivity for the entire country of Andorra.

In addition, IT and telecommunications organizations suffered a great deal of DDoS attacks in 2022, with many targeted for disruptive reasons. A small IT company in the US, “FlexBooker”, was attacked in January of 2022, and the DDoS attack that hit the company’s AWS servers, resulting in a data breach of 3.7 million records that later appeared on a dark web hacker forum. Various reports and sources indicate that 2022 saw a 110% rise in network-layer DDoS attacks against Telecommunications organizations. Network-layer attacks aim to overwhelm network infrastructure, IE, in-line routers and servers, and the Internet link itself. Many network-layer DDoS attacks were launched against organizations in the US, China, and Germany and according to reports, the main goal was to disrupt services, although one cannot rule out ransom-based attacks.

With many gaming companies launching new titles and long-awaited sequels in 2023, it is evident that such companies should put more emphasis on testing and diagnosing their dynamic DDoS attack surface to uncover their critical vulnerabilities. “Due to the dynamic nature of networks and services, DDoS protection is not aware of changes to the environments it is protecting, which leaves a large number of vulnerabilities hidden and unknown,” comments Matthew Andriani. “In recent years, and especially in 2022, many organizations and governments had no visibility into their critical vulnerabilities, leaving their attack surface completely exposed to DDoS attacks. This is natural, as these organizations have complex networks and an ongoing production schedule. But 2023 will show continuous evolution to these radical DDoS attacks. Organizations cannot stay on the sidelines and hope for the best – they must take a proactive approach in order to stay protected against these DDoS attacks”, concludes Andriani.



Source: Kaspersky

2023, in a nutshell:

Going through the data from 2022, and seeing the steep incline of DDoS attacks worldwide, one can only assume that 2023 is probably going to be the year when gaming companies become the leading target for DDoS attacks, alongside governments and financial institutions. As the war between Russia and Ukraine is not nearing its end, and as networks continue to evolve and become more complex, it is clear that a new approach is needed in order to continue ongoing operations with minimal disruption and downtime, for all organizations, worldwide.