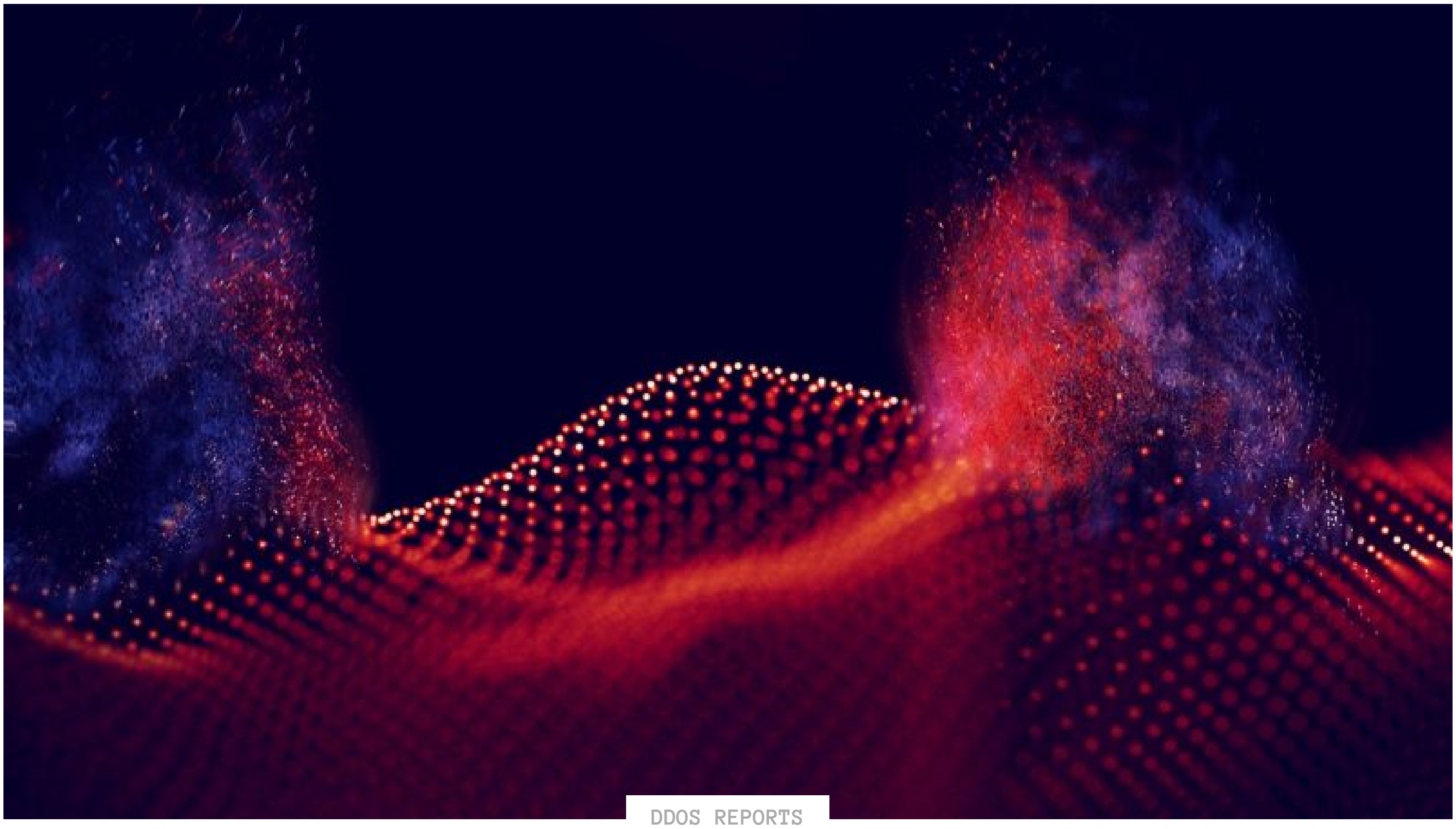


DDOS REPORTS

DDoS attacks in Q1 2022

25 APR 2022 ⌛ 14 minute read

News overview

The DDoS landscape in Q1 2022 was shaped by the ongoing conflict between Russia and Ukraine: a significant part of all DDoS-related news concerned these countries. In mid-January, the website of Kyiv Mayor Vitali Klitschko was hit by a DDoS attack, and the websites of a number of Ukrainian ministries were defaced. In mid-February, DDoS attacks affected the website of Ukraine's Ministry of Defense, online services of Oschadbank and PrivatBank, as well as the hosting provider Mirohost. Around the same time, PrivatBank customers received fake text messages about out-of-service ATMs, seemingly intended to sow panic. Another wave of DDoS engulfed Ukrainian government resources on February 23, while the State Service of Special Communication and Information Protection of Ukraine reported a series of continuous attacks in late February and early March. Although the volume of junk traffic exceeded 100 GB/s at peak onslaught, that pales in comparison to the attacks of 1 TB/s capacity or more that occured repeatedly last year.

In early March, researchers at Zscaler published an analysis of attacks on Ukrainian resources carried out by a DanaBot operator. This banking Trojan spreads via the malware-as-a-service (MaaS) model. The buyer used DanaBot to download onto infected devices a DDoS bot whose sole function was to attack a hard-coded domain. The initial target was the mail server of the Ukrainian Ministry of Defense. The attacks on this resource continued from March 2 through March 7, after which the cybercriminals switched to the page of the National Security and Defense Council of Ukraine website dedicated to information about Russian prisoners of war.

The information resource LiveUAMap, which provides real-time monitoring of the Russian-Ukrainian conflict, also became a DDoS target. This website is used by reporters and charities as a source of up-to-date information. In addition, Ukrainian media and information resources of NATO countries were subjected to attacks. In particular, the Ukrainian portal Espreso suffered a DDoS strike. According to Ukrainian providers, they faced DDoS attacks on certain resources throughout the whole of March.

Starting February 24, a spate of DDoS attacks hit Russian websites. The targets included media, government authorities at the regional (for example, in Yugra) and federal levels, Roscosmos, Russian Railways (RZD), the State Services (Gosuslugi) portal, telcos and other organizations. At the end of March, DDoSers went after the Russian domain registrar Ru-Center, disabling the websites of its customers for some time. According to RBC, at least some of the attacks targeting media were carried out from websites calling for an end to misinformation. The hacktivist group Anonymous, having declared war on Russia over Ukraine, claimed responsibility for several attacks, including a DDoS against the news station Russia Today.

Anonymous is not the only hacktivist group to come out in support of Ukraine. The country's government called upon volunteers to join the "IT army," whose tasks include DDoS attacks. Such attacks were coordinated primarily through Telegram, where the organizers posted lists of targets. Moreover, multiple websites appeared inviting sympathizers with any level of IT literacy to join the DDoS offensive against Russian organizations. All the user had to do was open the website in a browser for it to start sending junk requests to a given list of web resources. And to make it more entertaining, some stresser websites, for example, gamified the process.

Hacktivists also distributed apps allowing ordinary users to take part in DDoS attacks. As with the websites, their developers advertised them as tools for attacking Russian resources. According to Avast, one such app was downloaded by at least 900 users from Ukraine. Such apps do not just carry out attacks on behalf of users, but collect data about them, such as IP address, approximate location, username, system information, time zone, language, etc.

In response to the DDoS attacks, many Russian resources have employed geofencing to temporarily restrict access from abroad. In addition, Russia's National Coordination Center for Computer Incidents published lists of IP addresses and domains from which attacks were allegedly launched, plus security recommendations for organizations. The list of DDoS sources included, inter alia, the domains of US intelligence agencies, as well as some media outlets.

Besides Russian and Ukrainian resources, North Korean websites also became unavailable several times. The country first went offline in mid-January after a series of missile tests, cutting access to most North Korean websites and mail servers. Researcher Junade Ali, who monitors the North Korean internet, said the incident resembled a DDoS attack. On January 26, the story repeated itself — after more tests. Connectivity disruptions were observed in the country at the end of the month, too. Although many initially attributed the incidents to North Korea's increased military activity, it was an American infosec expert nicknamed P4x who claimed responsibility. In his own words, he acted in response to a series of cyberattacks by North Korean hackers against security experts. Seeing no reaction from the US authorities, P4x decided to take matters into his own hands: he found several vulnerabilities in North Korean network equipment which he used to overload critical routers and servers in the country.

In March, the Israeli ISP Cellcom was the target of a large-scale DDoS attack. The incident took government resources, in particular ministry websites, offline for some time. The attack also hit another major Israeli provider, Bezeq. The Israel National Cyber Directorate (INCD) believes that Iran was behind the attack.

Another DDoS-hit country is Andorra. The targeting of Andorra Telecom, the only local ISP, temporarily cut off communications for everyone in the country. The attackers' motive was far from political: the target seemed to be participants in the Twitch Rivals Squidcraft Games, a Minecraft tournament based on *Squid Game*. The tournament was for Spanish-speaking streamers in Europe and Latin America, and the top prize was $100,000. Among the players were many Spaniards living in Andorra — the attackers most likely wanted to disconnect them from the game. But because the country is small, its entire infrastructure was affected.

Q1 was not without DDoS attacks on suppliers of the popular technologies of blockchain and NFT. Right at the start of the year, the Solana platform, after repeated DDoS attacks in 2021, was hit again. The attackers disabled the platform using its own functionality by "spamming" the blockchain with empty transactions, causing the core network to overload and stop responding. This latest DDoS attack enraged users, who accused the developers of failing to secure the system.

No sooner had it opened than the new NFT marketplace LooksRare was DDoSed. The platform's website was temporarily down, and users had trouble connecting wallets and getting information about purchased tokens. The problems with wallets persisted for some time, even after access to the website was restored.

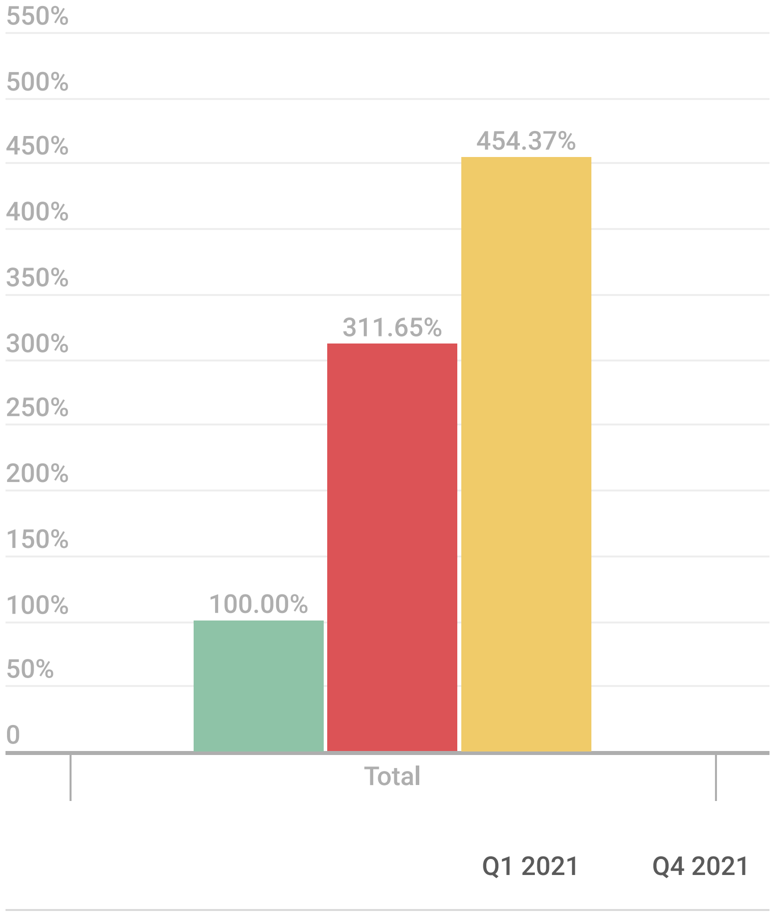
DDoS extortionists, posing as the infamous REvil group, not only continued to attack companies, but displayed creativity. Imperva reported attacks in which a ransom note was included in requests to the targeted website. What's more, if previously the attackers wanted a one-time ransom, they now demand 1 BTC per day in exchange for "protecting" the victim company from their attacks. Researchers note that the capacity of some attacks stretched to hundreds of thousands and even millions of requests per second. They also report that the attackers most likely used the Mēris botnet, discovered in Q3 2021.

In addition to requests carrying ransom notes, DDoS operators added another string to their virtual bow in Q1. Cybercriminals started using misconfigured Mitel MiCollab and MiVoice Business Express collaboration solutions to amplify attacks by more than 4 million times. Both solutions feature a TP-240 interface for VoIP. Acting as a bridge for interaction with this interface is the tp240dvr driver, whose tasks include receiving a command to generate huge amounts of traffic for the purpose of debugging and testing system performance. Normally this driver should not be available from the internet, but around 2,600 Mitel systems were found to accept commands from outside. The attackers forced vulnerable systems to send stress tests to the victim, thereby achieving manifold amplification. These attacks have been observed since mid-February and have targeted ISPs and financial, logistics and other organizations.

To combat DDoS and other cyberattacks, British authorities launched an initiative aimed at preventing child cybercrime. Students searching for suspicious terms on school computers see a warning page with a suggested redirection to information about cybercrime, its consequences and the Computer Misuse Act 1990. The pilot showed that in just four weeks children had become far less likely to search for “stressers” and “booters” (websites for carrying out DDoS attacks).

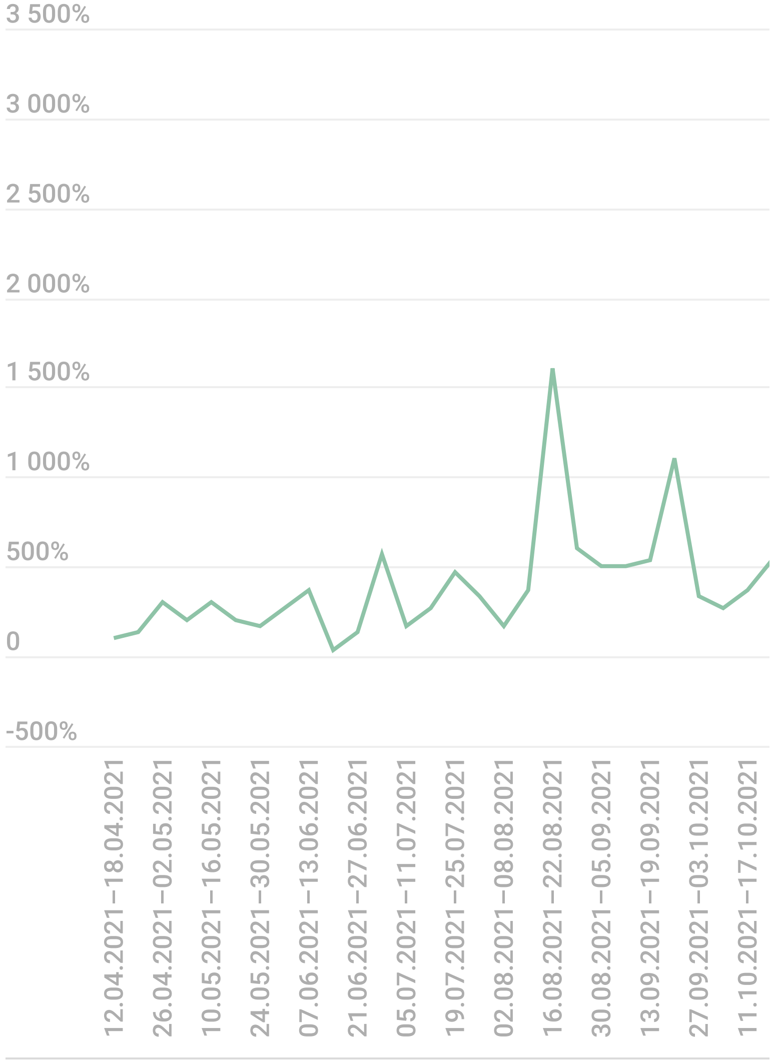
Quarter trends

Before evaluating the Q1 2022 data, it is worth recalling that our previous quarter report mentioned a record number of DDoS attacks. This quarter, we saw an almost 1.5-fold (46%) increase in the number of attacks relative to the record, and a 4.5-fold rise compared to the same period last year.



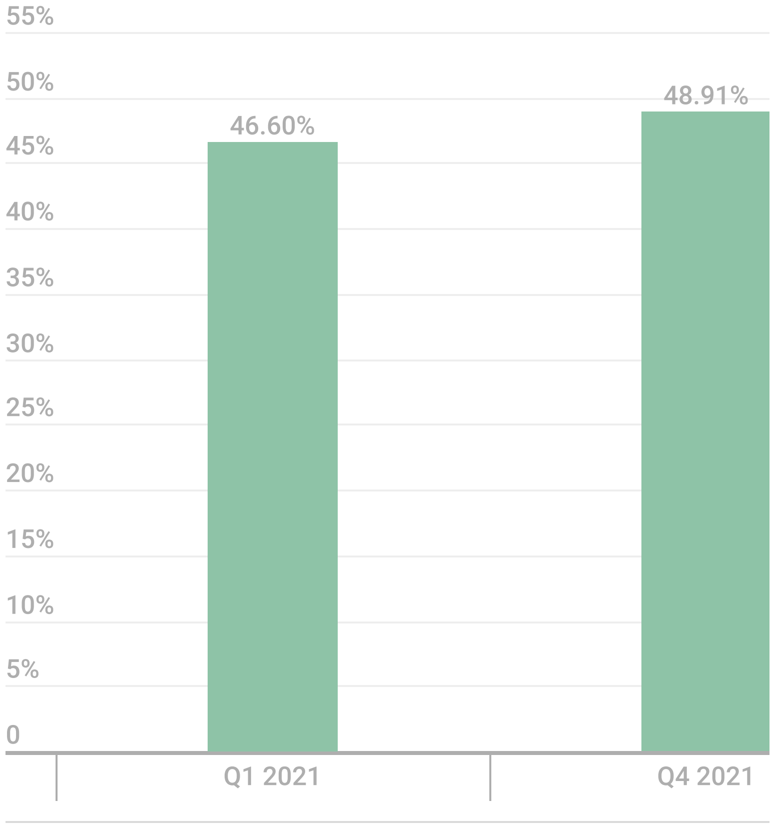
Comparative number of DDoS attacks, Q1 2022, Q1 and Q4 2021. Q1 2021 data is taken as 100% (download)

The reason for this growth is obvious: the crisis in Ukraine led to a cyberwar, which could hardly fail to impact the statistics. Looking at the distribution of DDoS attacks by week, we see that the peak of new attacks occurred in the eighth week of 2022, that is, February 21–27, and we repelled the largest number of DDoS attacks that week on February 25.



Comparative number of DDoS attacks by week, April 2021–March 2022 (download)

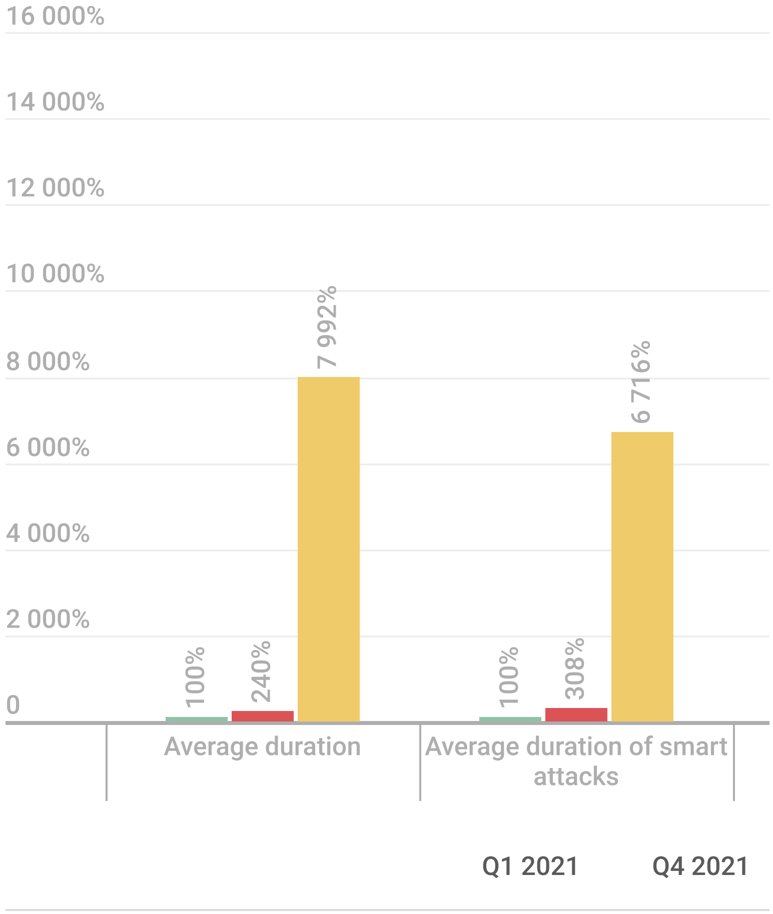
That said, there were relatively few attacks before late February, and without the spike in DDoS activity at the end of the month we would have seen a drop relative to the previous quarter. It is interesting to note that very many of the attacks in late February/early March were organized by hacktivists and carried out from personal devices that users voluntarily connected to the botnet (for example, by opening a stresser website in their browser).



Share of smart attacks, Q1 2022, Q1 and Q4 2021. The Q1 2022 decrease in this value is due to the surge in hacktivism (download)

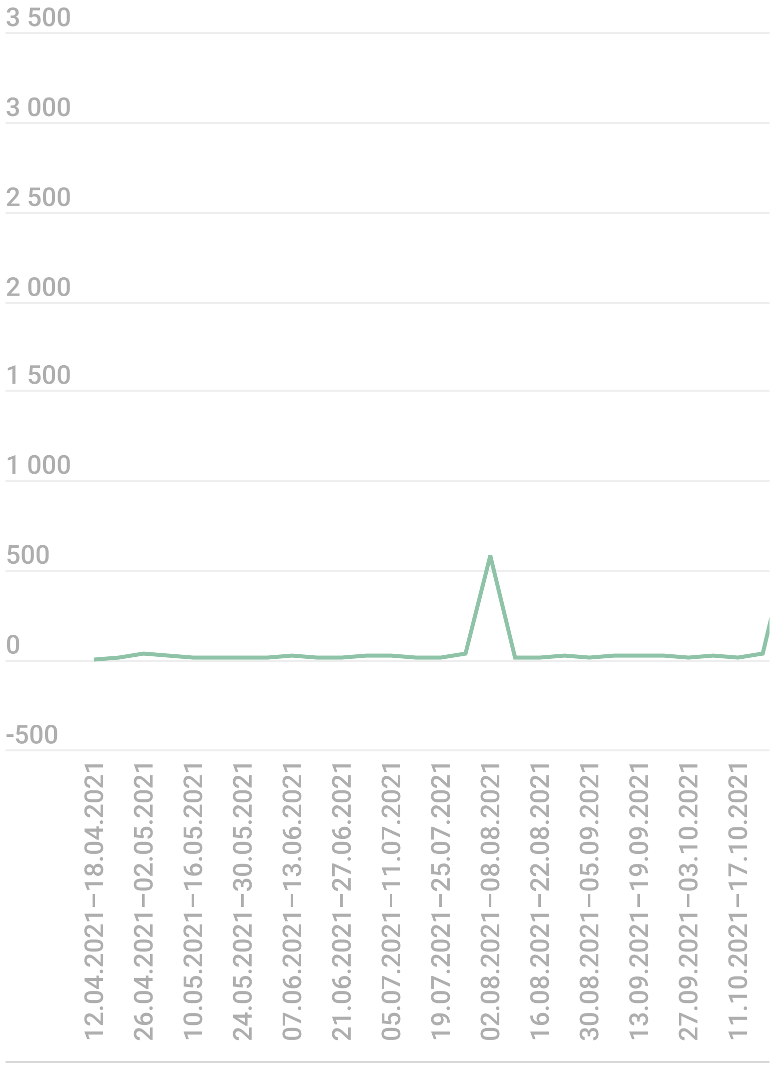
The hacktivist nature of the attacks was also responsible for the sharp decline in their number towards mid-March: those initially driven by emotion had calmed down, and infosec companies published warnings against taking part in such attacks. As a result, the number of hacktivists decreased. Whereas in late February/early March we saw an unusually high number of amateurs involved in the attacks, by the end of March their relative number had almost returned to normal levels. In absolute terms, there are still more of them than usual, as well as of DDoS attacks, but the difference is not so great.

But the most curious thing has to do with the data not on the number of attacks, but on their duration. In Q1 we saw an increase in this indicator by two orders of magnitude. If previous attacks were measured in minutes, now the average attack is measured in hours, and many go on for several days. We detected the longest attack on March 29, which lasted a little over 177 hours, that is, more than a week.



DDoS attack duration, Q1 2022, Q1 and Q4 2021. Q1 2021 data is taken as 100% (download)

This is extremely uncharacteristic of DDoS attacks, especially ones filtered by security solutions. Attacks of this length are expensive and expose the botnet, since active nodes are easier to detect and disable. So professional DDoSers always try to stop an ineffective attack as quickly as possible so as not to waste money. Now, however, we are seeing the opposite: attacks continue regardless of their effectiveness. At the same time, the overwhelming majority of targets of ultra-long (more than a day) attacks are government agencies and banks. All of this underscores once more that many of the DDoS attacks this quarter were not financially motivated.



Average DDoS attack duration by week, April 2021–March 2022. A sharp increase occurs in the last third of February (download)

The upswing in DDoS attacks in Q1 2022 led to another significant trend: many Russian organizations were unprepared for being targeted. As a result, both we and other anti-DDoS protection providers received a huge number of requests in a short space of time from companies already under attack.

DDoS attack statistics

Methodology

Kaspersky has a long history of combating cyberthreats, including DDoS attacks of any type and complexity. Company experts monitor botnets using the Kaspersky DDoS Intelligence system.

A part of Kaspersky DDoS Protection, the DDoS Intelligence system intercepts and analyzes commands received by bots from C2 servers. The system is proactive, not reactive, meaning that it does not wait for a user device to get infected or a command to be executed.

This report contains DDoS Intelligence statistics for Q1 2022.

In the context of this report, the incident is counted as a single DDoS-attack only if the interval between botnet activity periods does not exceed 24 hours. For example, if the same resource is attacked by the same botnet after an interval of 24 hours or more, two attacks will be counted. Bot requests originating from different botnets but directed at one resource also count as separate attacks.

The geographic locations of DDoS-attack victims and C2 servers used to send commands are determined by their respective IP addresses. The number of unique targets of DDoS attacks in this report is counted by the number of unique IP addresses in the quarterly statistics.

DDoS Intelligence statistics are limited to botnets detected and analyzed by Kaspersky. Note that botnets are just one of the tools used for DDoS attacks, and that this section does not cover every single DDoS attack that occurred during the review period.

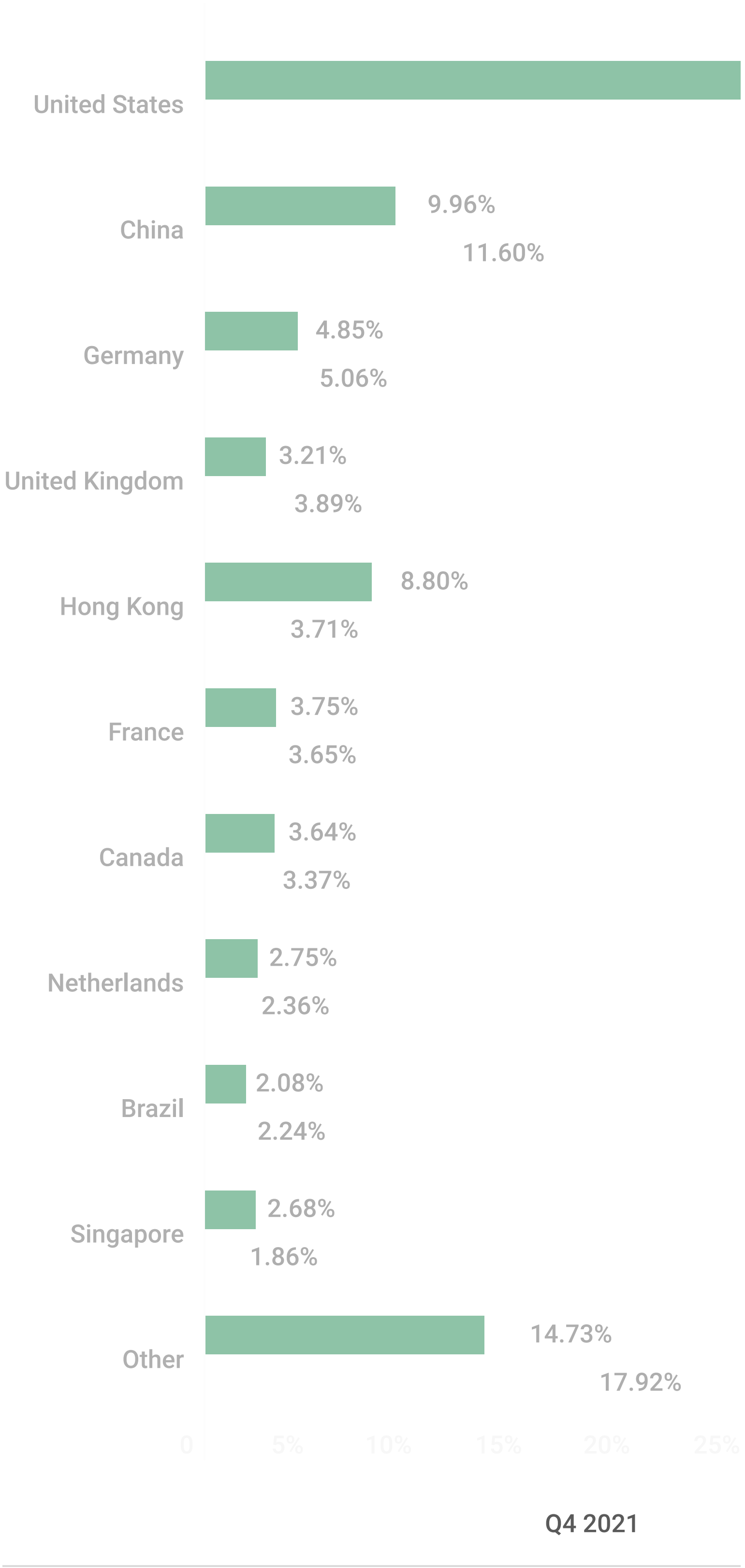
Quarter summary

In Q1 2022:

- Kaspersky DDoS Intelligence system detected 91,052 DDoS attacks.
- 44.34% of attacks were directed at targets located in USA, which comprised 45.02% of all targets.
- The largest number of DDoS-attacks (16.35%) come on Sundays.
- Most attacks (94.95%) lasted less than 4 hours, but the longest attack continued for 549 hours (nearly 23 days).
- 53.64% of attacks were UDP flood.
- 55.53% of C&C servers were located in USA.
- China accounted for 20.41% of bots attacking our SSH honeypots and 41.21% of those attacking Telnet traps.

DDoS attack geography

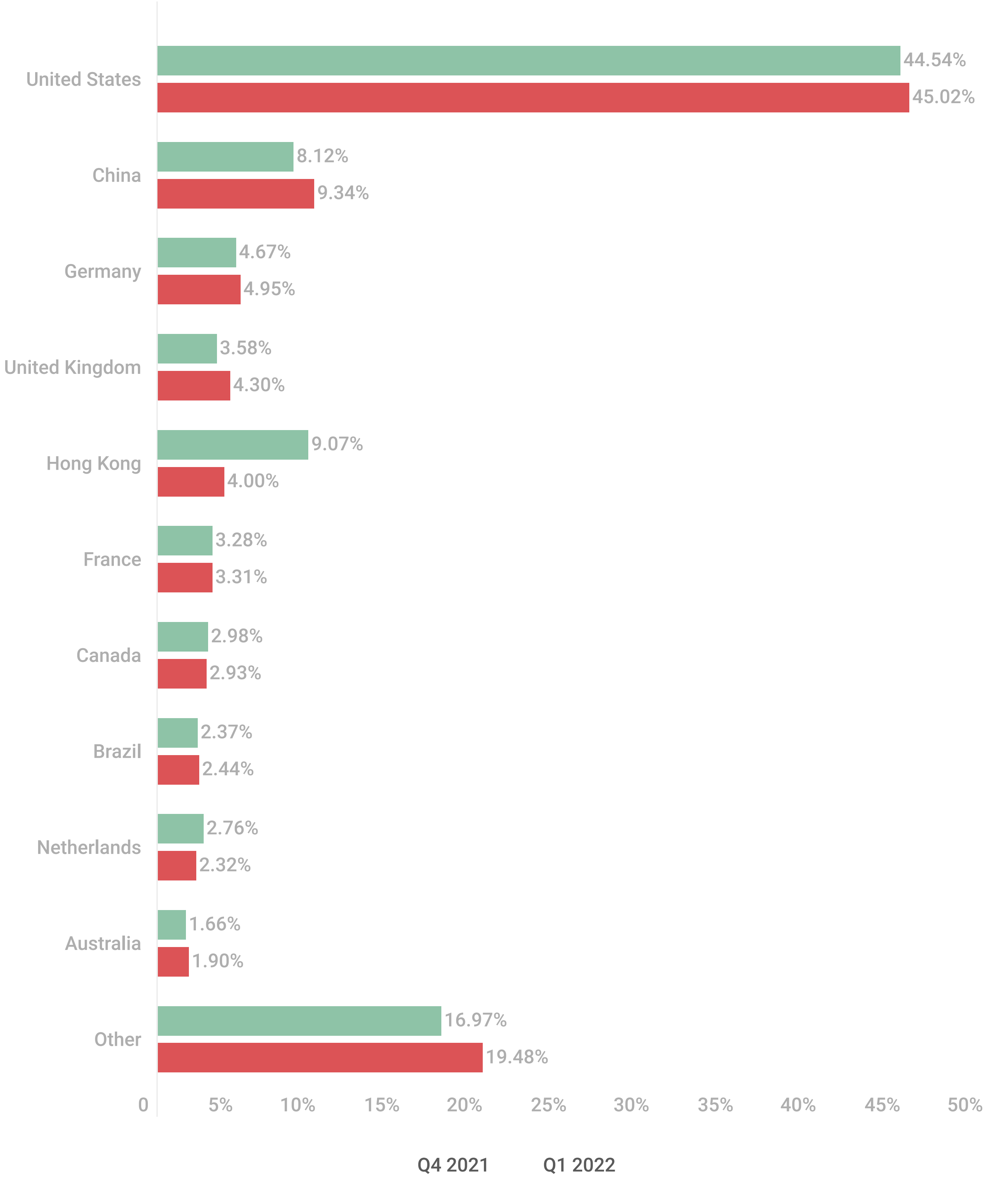
In Q1 2022, US-based resources were most frequently hit by DDoS attacks (44.34%). Their share increased slightly against the previous reporting period. In second place remains China (11.60%), whose share also rose slightly, and Germany (5.06%) moved into third.



Distribution of DDoS attacks by country and territory, Q4 2021 and Q1 2022 (download)

The Hong Kong SAR (3.71%) saw its share more than halve, taking fifth place by number of DDoS attacks in Q1. The UK (3.89%), which added 0.68 p.p., finished fourth. France (3.65%) and Canada (3.37%) dropped to sixth and seventh, respectively, while the Netherlands (2.36%) remained in eighth position. Brazil (2.24%) and Singapore (1.86%) swapped places, coming in ninth and tenth, respectively. Overall, the geographical distribution of DDoS attacks changed little compared to Q4 2021.

The distribution of unique targets by country and territory traditionally mirrors the attack geography — only the bottom of the TOP 10 differs. Most targets in Q1 were located in the US (45.02%), followed by China (9.34%) and Germany (4.95%). The shares of the three countries have seen slight growth since the end of 2021. In fourth place is the UK (4.30%), and in fifth is Hong Kong (4.00%), whose share more than halved.

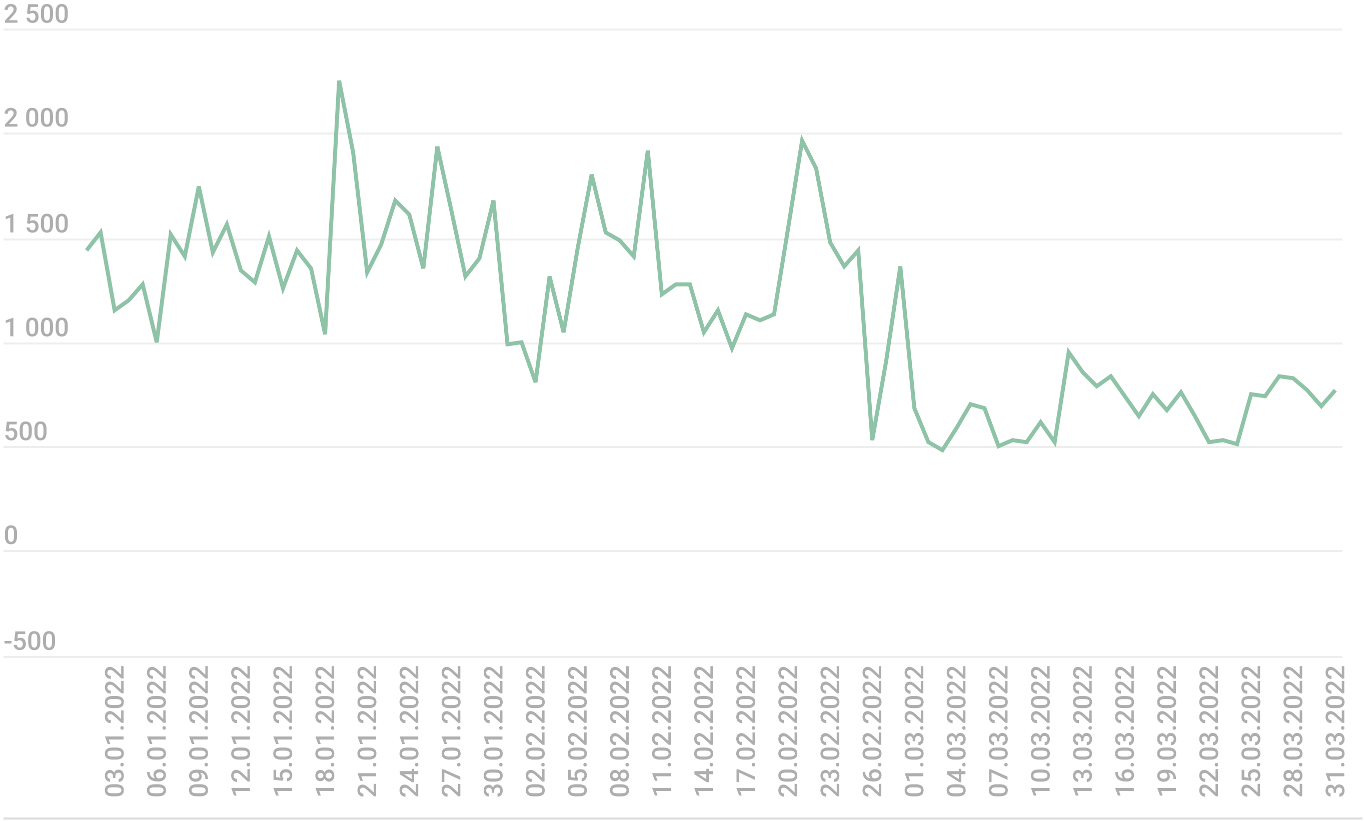


Distribution of unique targets by country and territory, Q4 2021 and Q1 2022 (download)

France (3.31%) and Canada (2.93%) remained in sixth and seventh positions, respectively, while Brazil (2.44%) moved up to eighth. By contrast, the Netherlands dropped to ninth place (2.32%). Australia (1.90%) rounds out the TOP 10.

Dynamics of the number of DDoS attacks

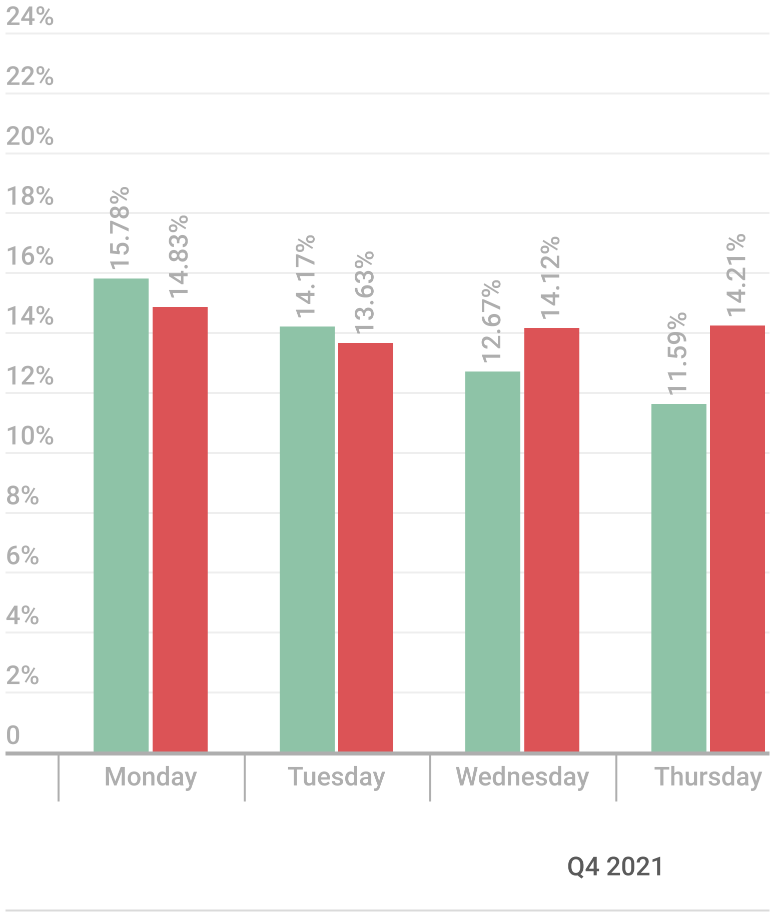
In Q1 2022, our DDoS Intelligence system detected 91,052 DDoS attacks. Throughout January and most of February, we saw an average of 1,406 attacks per day. The calmest day of this period was February 2, when DDoS Intelligence detected 809 attacks, and the stormiest was January 19, when 2,250 DDoS attacks were recorded. Since February 26, the average number of DDoS attacks per day has halved to 697. The most active day at the end of the quarter was February 28 with 1,362 attacks, and the quietest was March 3 with 479. Note that attacks by spontaneous hacktivist botnets, which happened to surge in late February and March, are not monitored by DDoS Intelligence.



kaspersky

Dynamics of the number of DDoS attacks, Q1 2022 (download)

The distribution of DDoS attacks by day of the week is slightly more evenly spread than in Q4 2021. The difference between the most active and the quietest days was 3.58 p.p. The largest share of attacks, as in the previous reporting period, came on Sunday (16.35%), and the lowest on Friday (12.77%), which in late 2021 was quite an active day. The shares of both days of the week fell.

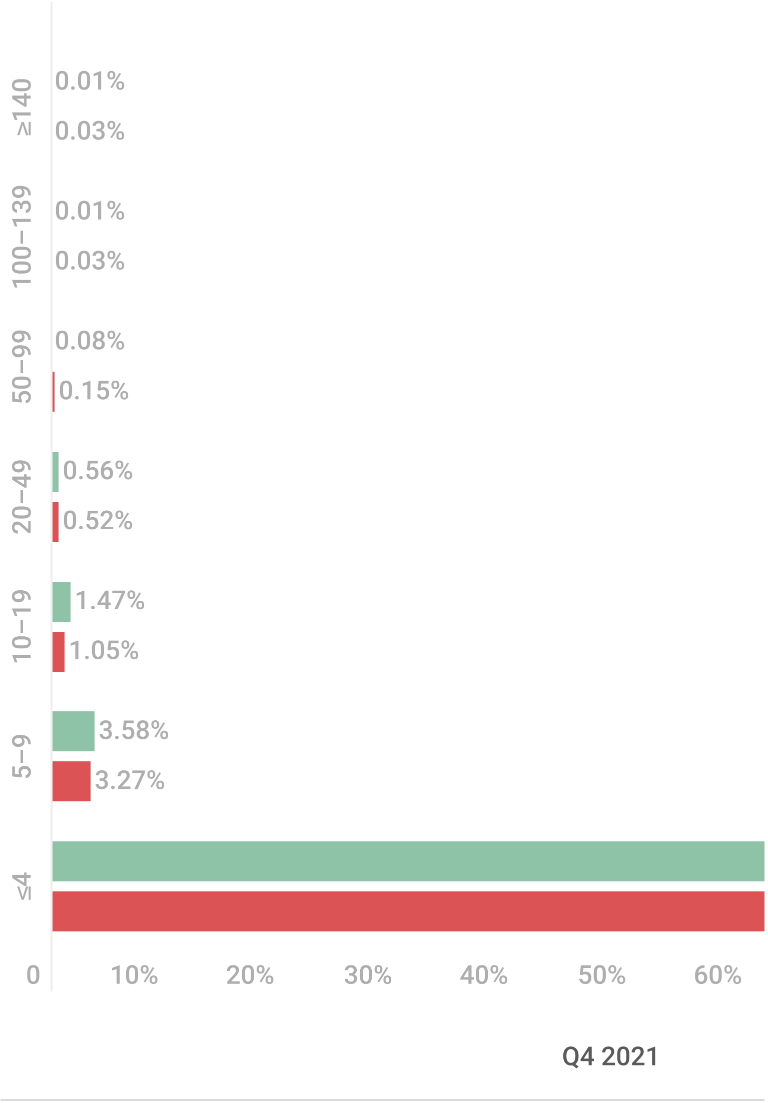


Distribution of DDoS attacks by day of the week, Q1 2022 (download)

Besides Friday and Sunday, Monday (14.83%), Tuesday (13.63%) and Saturday (14.09%) were calmer, while the shares of Wednesday (14.12%) and Thursday (14.21%) increased.

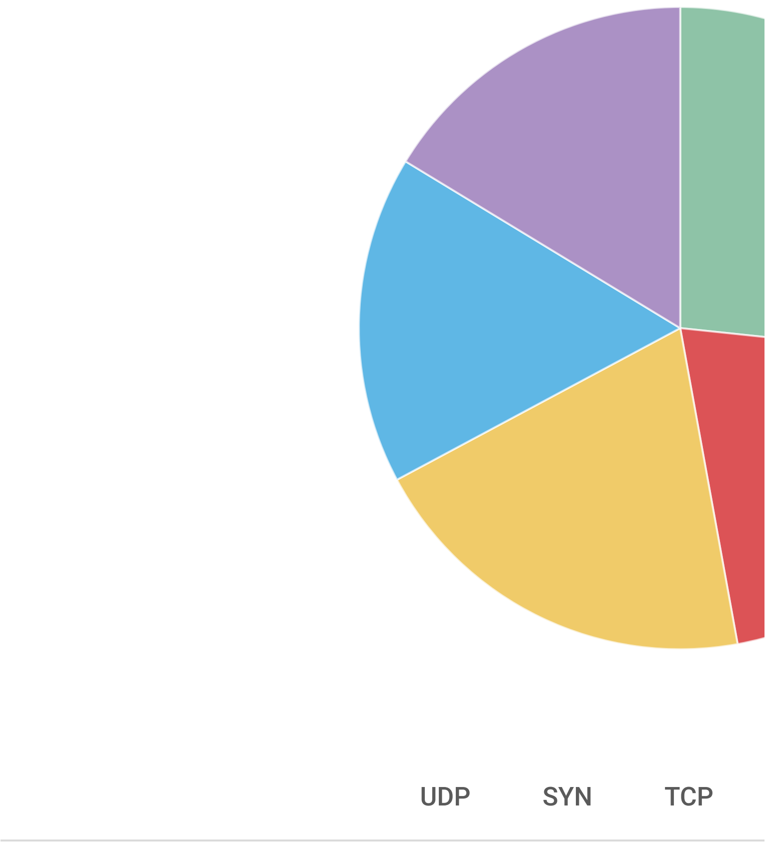
Duration and types of DDoS attacks

The average DDoS attack duration in the first three months of 2022 remained at the same level as in Q4 2021 — just under two hours. At the same time, the proportion of both very short (94.95%) and long attacks increased: DDoS attacks lasting more than 140 hours accounted for 0.03%, as did those lasting 100–139 hours. The share of attacks lasting 50–99 hours climbed to 0.15%. The duration of the quarter's longest attack also increased: from 218 to 549 hours. Conversely, the share of moderately short attacks (5–49 hours) decreased.



Distribution of DDoS attacks by duration, Q4 2021 and Q1 2022 (download)

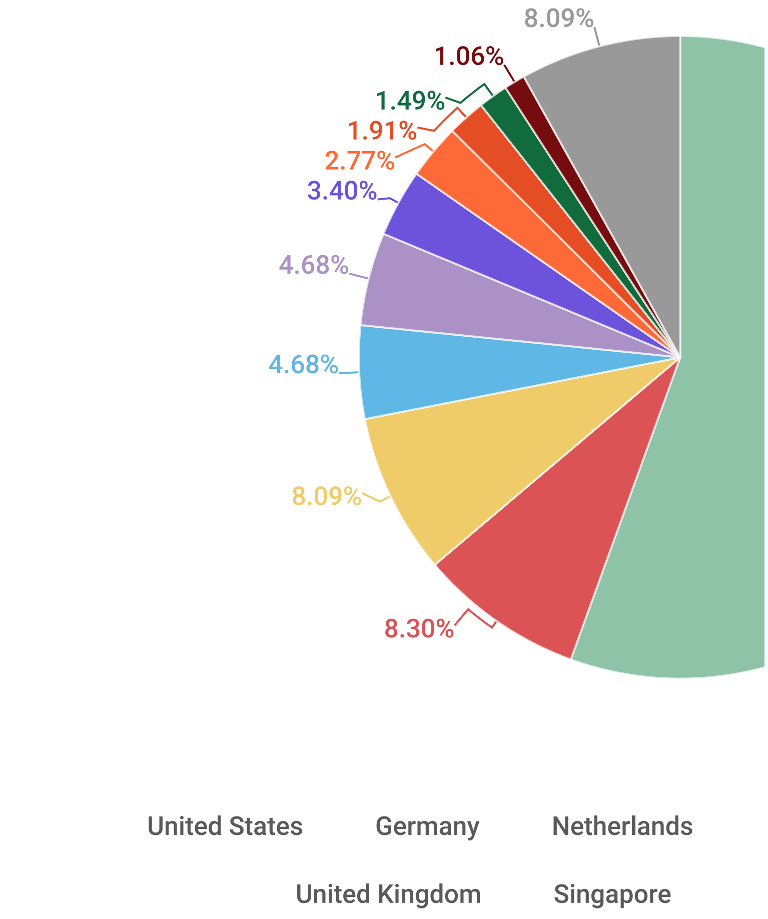
UDP flooding (53.64%) constituted more than half of all DDoS attacks in Q1, adding 3.33 p.p. SYN flooding (22.37%) moved up to second, adding 6.08 p.p., while TCP flooding (20.17%) saw its share cut by a third, relegating this type of DDoS to third place. HTTP flooding (2.42%) and GRE flooding (1.41%) marginally increased their shares, but remained in fourth and fifth, respectively.



Distribution of DDoS attacks by type, Q1 2022 (download)

Geographic distribution of botnets

Glancing at the geographic distribution of botnet C&Cs, we see that more than half of those active in Q1 were located in the US (55.53%), up 9.04 p.p. from the end of 2021. Germany (8.30%) moved into second place (8.30%), followed by the Netherlands (8.09%). The Czech Republic (4.68%) and Russia (4.68%) share fourth place.

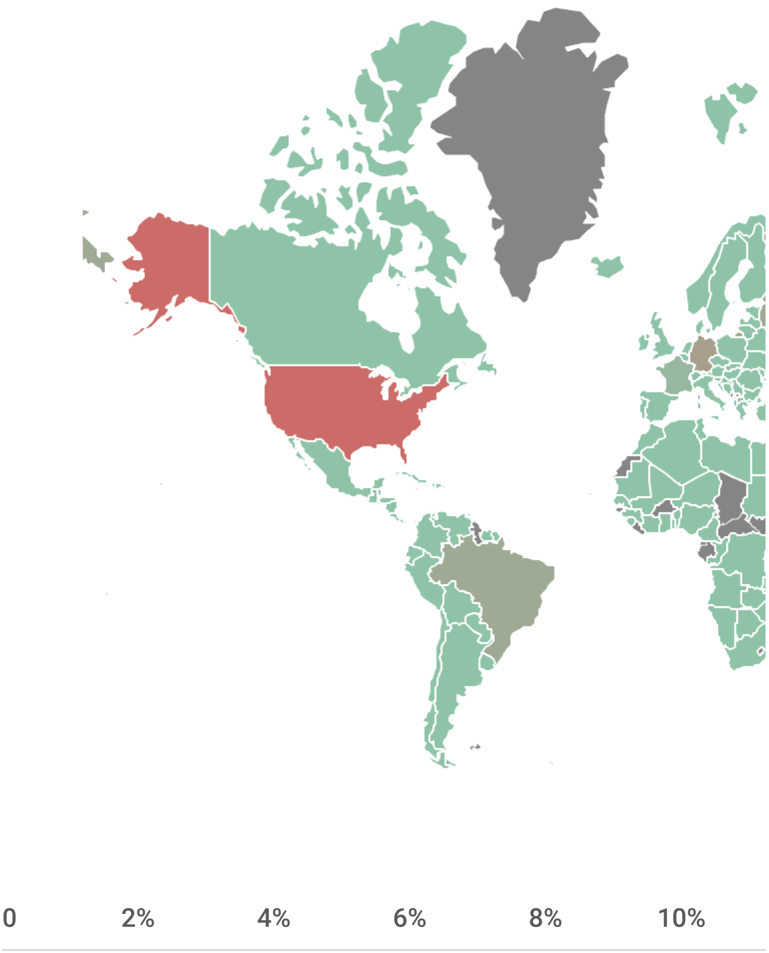


Distribution of C&C botnet servers by country, Q1 2022 (download)

In sixth place by number of C&C servers in Q1 is France (3.40%), in seventh is the UK (2.77%), and propping up the TOP 10 is Canada (1.06%). Eighth and ninth positions were taken by countries that did not make the TOP 10 last quarter: Singapore (1.91%) and India (1.49%).

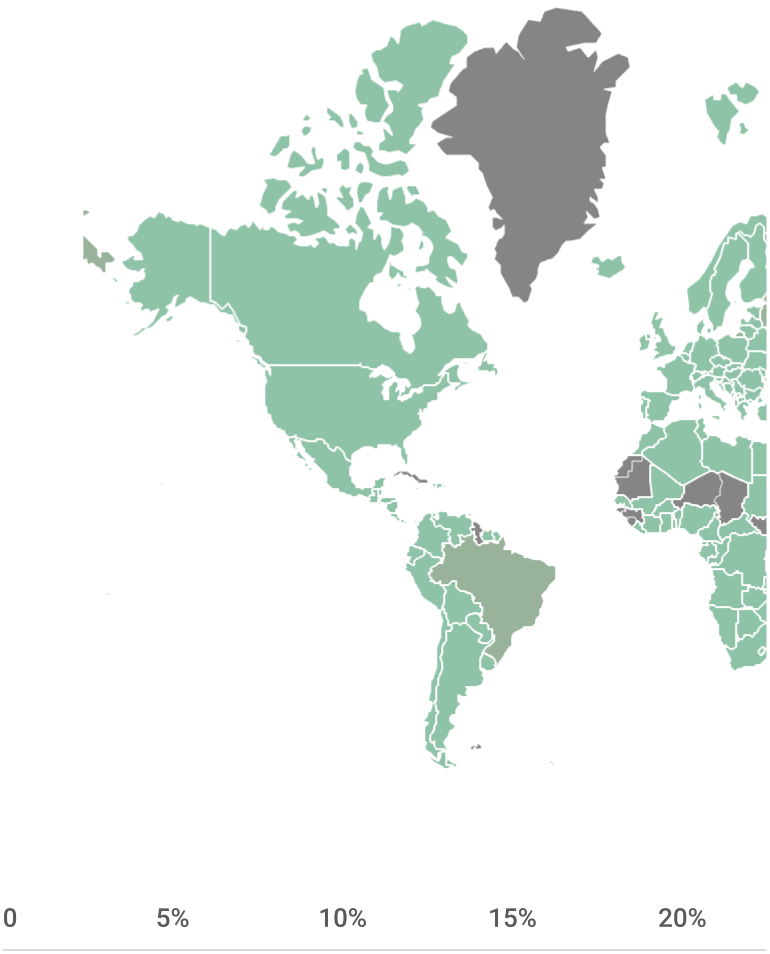
Attacks on IoT honeypots

The largest share of bots trying to hack into our SSH honeypots in Q1 fell to China (20.41%). That said, the country's share decreased compared to the previous reporting period by 6.32 p.p.; meanwhile, the share of the US rose from 11.20 to 15.24%. In third place in the list of countries and territories from which attacks originated is Germany (7.05%), followed by Brazil (4.91%) and Hong Kong (4.79%). However, not all bots were equally active. For instance, almost half of the attacks on our honeypots came from Russia (47.23%), despite accounting for just 3.40% of the total number of bots. In turn, China and the US were responsible for 9.01% and 8.16% of attacks, respectively.



Geographic distribution of devices from which attempts were made to attack Kaspersky SSH honeypots, Q1 2022 (download)

The ranking of countries and territories with the most devices trying to hack into our Telnet honeypots is likewise headed by China (41.21%). Its share dropped since the last quarter, but remains significantly higher than that of other countries. India (8.44%) and Russia (6.15%) remained second and third, followed by Brazil (5.36%) and the US (3.95%). Meanwhile, Chinese bots were responsible for almost two-thirds (65.48%) of all attacks on Telnet honeypots, and another 12.02% of attacks came from inside the US.



Geographic distribution of devices from which attempts were made to attack Kaspersky Telnet honeypots, Q1 2022 (download)

Conclusion

The DDoS attack landscape in Q1 was strongly influenced by the geopolitical situation: since the end of February, we have seen a surge in hacktivist activity and the emergence of a large number of spontaneous botnets that users connected to voluntarily. Hacktivist attacks were notable for their length, even if security solutions successfully filtered out the junk traffic. At the same time, known botnets, which we have long been monitoring, became far less active from late February, while in terms of duration, the number of both long and very short attacks of these botnets increased against the previous reporting period.

The Q1 situation with anti-DDoS protection in Russia warrants a separate mention. As we have said repeatedly, cyberdefenses need deploying in advance, because when an attack comes, it will be too late. This is precisely what very many owners of Russian network resources encountered at the end of February. The wave of new customers overwhelmed anti-DDoS services in the country. There was simply not enough time to set up protection, which led to long downtime for many resources. You never know when emergency occurs, so if you have yet to take care of anti-DDoS protection, we recommend that you start today.

It is very hard to predict anything in the current climate. The only certainty is that the state of the DDoS market in Q2 will depend directly and primarily on geopolitics. It is highly unlikely that we will see a decline in DDoS activity before the end of hostilities in Ukraine. Yet neither do we expect growth in Q2: for there to be a DDoS surge like we observed in late February/early March, a new shock of global proportions is needed.

BOTNETS CYBERCRIME DDOS-ATTACKS INTERNET OF THINGS

Authors

Expert ALEXANDER GUTNIKOV Expert OLEG KUPREEV Expert YAROSLAV SHMELEV