DDOS REPORTS

DDoS attacks in Q4 2021

10 FEB 2022 14 minute read

News roundup

Q4 2021 saw the appearance of several new DDoS botnets. A zombie network, named Abcbot by researchers, first hit the radar in July, but at the time it was little more than a simple scanner attacking Linux systems by brute-forcing weak passwords and exploiting known vulnerabilities. In October, the botnet was upgraded with DDoS functionality. Then in December, researchers at Cado Security linked the botnet to the Xanthe cryptojacking group. This is further evidence that the same botnets are often used for mining and DDoS.

The EwDoor botnet, which first came to researchers' attention in late October, turned out to be more picky than Abcbot. This zombie network consists solely of EdgeMarc Enterprise Session Border Controller devices located on AT&T carrier networks. The bot infiltrated the devices through the CVE-2017-6079 vulnerability, which allows execution of arbitrary commands. By exploiting a bug in the bot itself (one of the first versions accessed a non-existent C2 server registered by researchers), Netlab 360 managed to detect 5,700 infected devices. However, the cybercriminals later severed communication with this server. AT&T is investigating attacks on EdgeMarc devices.

In November, Qrator Labs recorded a series of short but powerful attacks on its systems and those of its clients. The attackers used a TCP data flood: they established a TCP connection to the victim's

server, then flooded it with random heavy TCP packets. In some cases, DNS amplification was also used. The attacks, launched from thousands of cameras and routers, lasted 2–3 minutes and then stopped. Researchers note that the botnet is new, and they currently lack sufficient data to describe it. They also speculate that the short attack duration is because the attackers wish to remain undetected, so they do not borrow infected device users' communication channels for long.

Google's Damian Menscher discovered a zombie network consisting of vulnerable GitLab servers. The botnet hijacked new devices by exploiting the CVE-2021-22205 vulnerability, which GitLab patched in April 2021, and carried out DDoS attacks of over 1TB/s. Menscher does not specify whether the bot is entirely new or related to existing botnets. However, around the same time, Cloudflare reported a brief but powerful Mirai-type attack, involving, among other things, GitLab servers infected through CVE-2021-22205.

Known botnets made the news more than once in Q4. For instance, Moobot added a relatively fresh vulnerability to its arsenal. A bug designated as CVE-2021-36260 was found in some Hikvision camera models and patched in September 2021. Like CVE-2017-6079, this vulnerability allows attackers to execute arbitrary commands. Once on the device, Moobot waits for a command from the C2 server before launching a DDoS attack. Researchers link the campaign to a DDoS-as-a-Service provider whose Telegram channel they came across during their analysis. The channel was created in June and went live in August 2021.

The Mēris botnet discovered last quarter turned out to be two botnets, reports Netscout. The company named the second one Dvinis ("twin" in Latvian). Unlike its elder brother, it does not use HTTP pipelining, but is also deployed in high-power attacks. Moreover, according to Netscout, Dvinis accounts for 75% of all attacks attributed to Mēris.

In late 2021, news broke of a vulnerability in the Apache Log4j library, which laid claim to being the most dangerous vulnerability of the year. Log4Shell, as the vulnerability is called, is present in all versions of Log4j from 2.0-beta9 to 2.14.1, and allows an attacker to take full control over a vulnerable system. What's more, an exploit for the vulnerability is available online, and the library that contains it is used in millions of products, both commercial and open-source. Not surprisingly, many cybercriminals, including DDoS botnet developers, have added Log4Shell to their toolkit. In particular, Mirai, Muhstik and Elknot bots are trying to exploit this vulnerability.

As for DDoS attacks themselves, media in the Philippines came under repeated fire during the past quarter. In mid-November, the online outfit PinoyMedia Center was flooded; then in the first half of December the same fate befell the news portal ABC-CBN News, followed by the media organization VERA Files; the digital media company Rappler was also attacked several times a month by unknown actors. Also in Q4, the Indonesian journalism initiative Project Multatuli got DDoSed after publishing an article criticizing the work of local law enforcement agencies.

Cybercriminals also targeted tech companies this quarter. The Polish arm of T-Mobile reported the largest ever attack on this sector in the country, which, however, was repelled. Another DDoS target was the blockchain platform Solana. Blockasset, an NFT marketplace powered by Solana, was the first to draw attention to the attack. The company noted that the DDoS had caused a slowdown in token distribution. GenesysGo, a Solana-based infrastructure provider, also noted some services were working intermittently, but assured there was no major cause for concern.

The DDoS attacks on VoIP providers continued. In early October, British company VoIP Unlimited fell victim again, having been attacked by DDoS extortionists last quarter. The new wave of junk traffic was accompanied by a ransom demand. Similar attacks affected various other British providers. And in November, clients of VoIP provider Telnyx worldwide were hit by outages. The perpetrators could be the REvil group, which is linked to past attacks on VoIP providers and was liquidated by Russian law enforcement agencies in January, after the US authorities had supplied information about the attackers.

In Q4, besides VoIP providers, e-mail service providers were targeted by ransom DDoS (RDoS) campaigns. Those affected were mostly small companies that provide secure and private e-mail accounts by subscription or invitation: Runbox, Posteo, Fastmail, TheXYZ, Guerrilla Mail, Mailfence, Kolab Now and RiseUp. The attackers called themselves Cursed Patriarch and demanded a ransom of 0.06BTC from victims (around US$4,000 at the time of the attack).

Ransomwarers continued to use DDoS as additional leverage. For instance, right from the start the new Yanluowang ransomware threatens to DDoS victims if "they take the attackers for fools." Besides Yanluowang, the HelloKitty ransomware group, known for attacking CD Projekt, the developer of *The Witcher* and *Cyberpunk 2077*, added DDoS to its arsenal.

Speaking of games: attackers in Q4 did not leave gamers alone. In October, *Apex Legends* players set a record for the longest match ever, because the server was DDoSed throughout. And attacks on Blizzard in November and December led to problems with accessing certain games, in particular *Overwatch* and *World of Warcraft*. Players themselves also got it in the neck. Among those who suffered were several popular streamers, likely due to an IP leak from the new title *Crab Game*: the streamers experienced issues after playing the game. Meanwhile, some *Dead by Daylight* streamers were not only DDoSed, but doxxed and swatted (the act of making a false report to the police with the intention of having a real-life SWAT team sent to the target's home). One of the victims tweeted that, during such a fake call, one of the police officers recognized him because he himself plays *Dead by Daylight*. How exactly the attackers got hold of the streamers' IP addresses and other data is unknown.

https://twitter.com/Elix_9/status/1458330303437574149

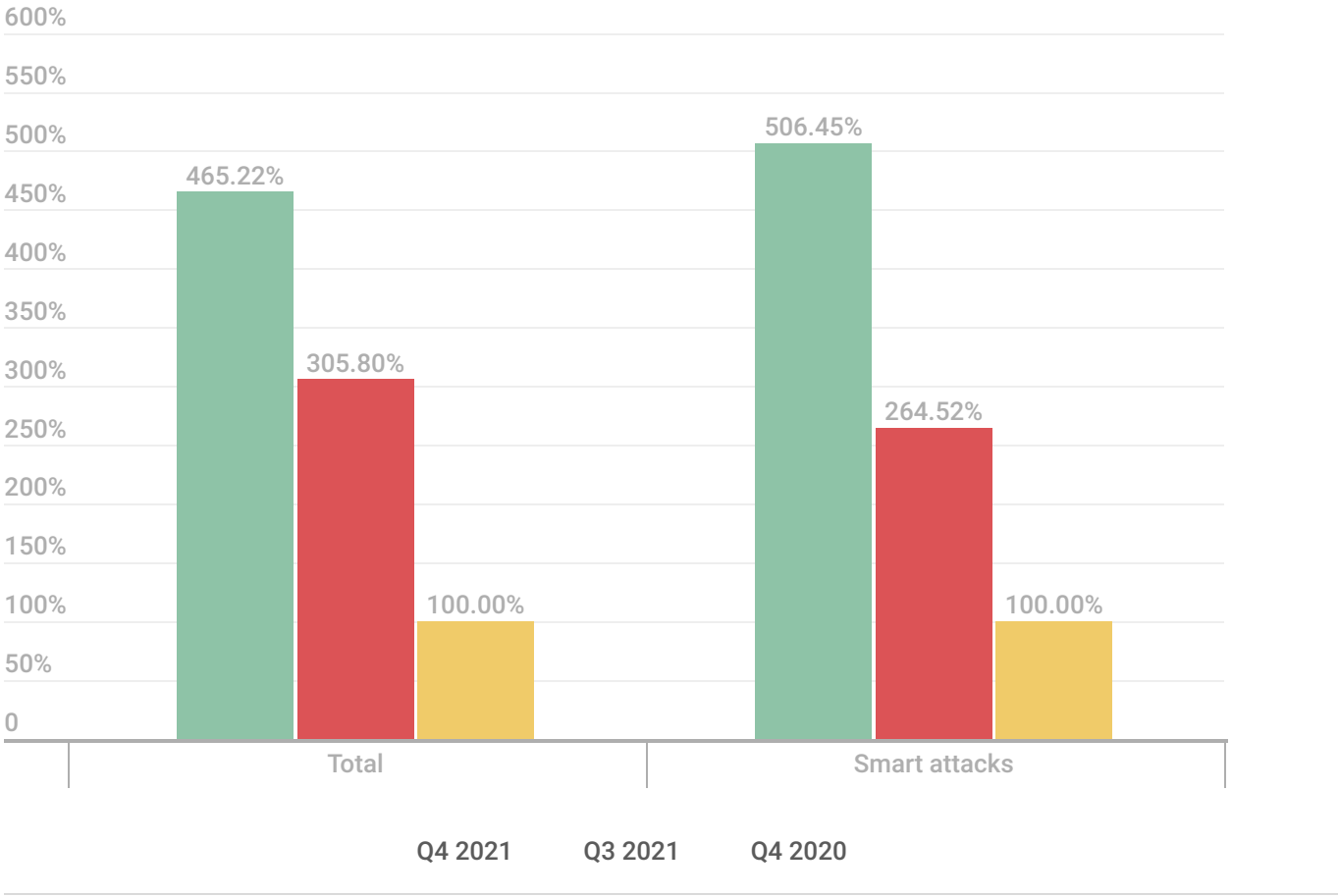
Fans of *Titanfall 2*, fed up with DDoS attacks, took the initiative in Q4 and created a mod for playing on custom servers if the official ones are down. Tracking the IP of a private server to flood it with junk traffic is not child's play, so this measure greatly reduces the likelihood of DDoS.

Successes in the fight against botnets were reflected in Q4 news. In October, for instance, Ukrainian police arrested the operator of a DDoS botnet consisting of 100,000 infected devices. And in December, Google filed a lawsuit against the operators of another botnet, Glupteba. The Internet giant also took steps to eliminate the botnet itself by blocking 63 million malicious documents, 908 cloud projects, more than a thousand Google accounts and a further 870 Google Ads accounts. Google also worked with other companies to shut down the botnet's C2 servers. Glupteba consists of a million infected IoT devices and Windows computers. The botnet can also install proxy servers on infected devices, mine cryptocurrency and conduct DDoS attacks. In addition, Glupteba uses the Bitcoin blockchain to store the addresses of backup C2 servers, making it harder to defeat. According to Kaspersky, it was this botnet that facilitated the spread of the notorious Mēris last quarter.

One last thing, attackers regularly carry out DDoS attacks on each other. In November, unknown actors tried to take down the dark-web marketplace Cannazon, which, as the name suggests, specializes in the sale of cannabis. The resource was shut down shortly afterwards, but its administrators claim they had long planned to close it anyway, and the DDoS was a convenient pretext to act sooner rather than later.

Quarter and year trends

Q4 played out in line with our forecasts: we saw impressive growth in the number of DDoS attacks, setting a new record in the history of our observations. Let's look at the figures:



kaspersky

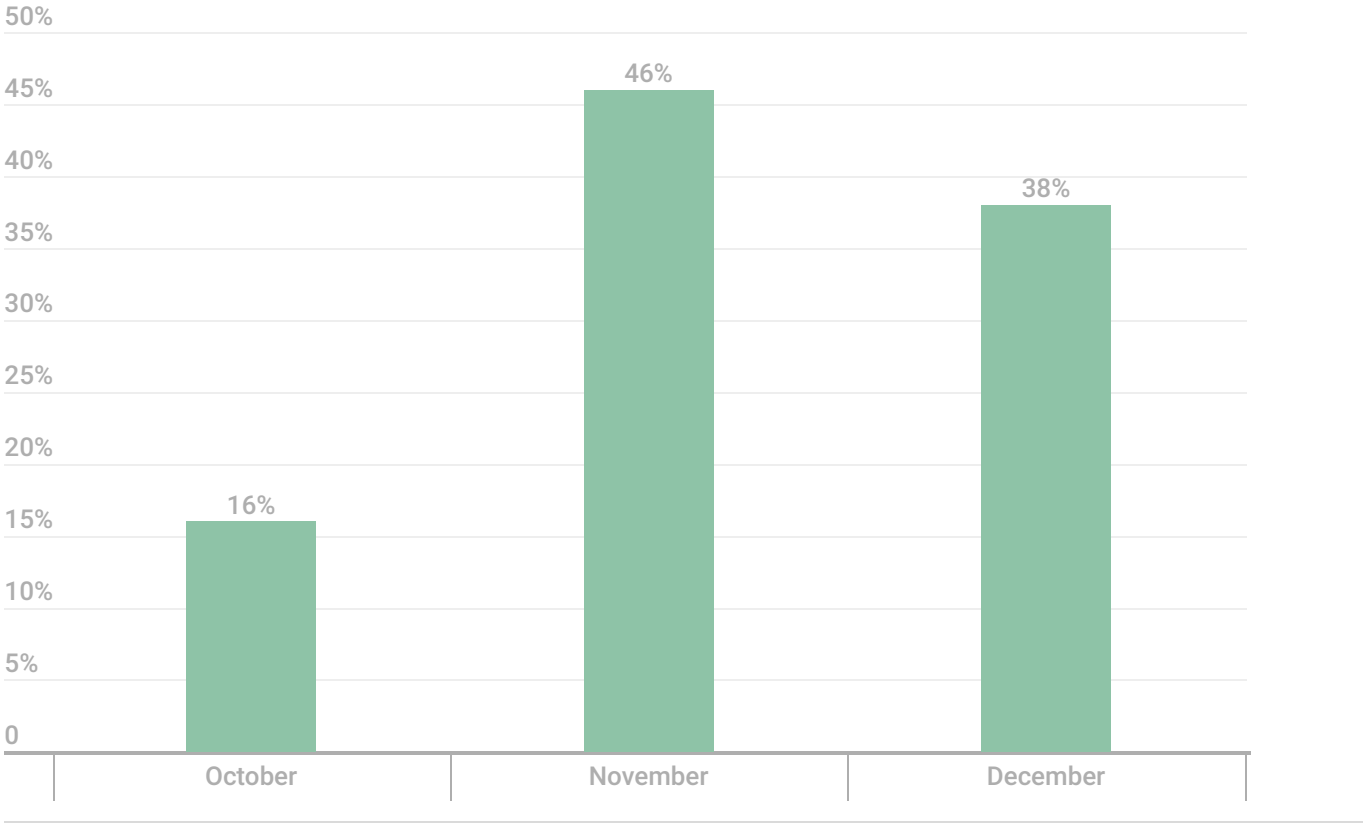
Comparative number of DDoS attacks, Q3 and Q4 2021, and Q4 2020. Q4 2020 data is taken as 100% (download)

The number of attacks in Q4 increased by 52% against the previous quarter and more than 4.5 times against the same period last year. The numbers look scary, but instead of rushing to conclusions, better to figure out why they are so.

Let's start with the increase in the number of DDoS attacks relative to Q3. Such growth in the last three months of the year is a traditional seasonal fluctuation that we predict (and that occurs) pretty much every year. Towards the end of the year, life steps up a gear, and this cannot fail to affect the DDoS market: competition in retail hots up, students sit exams, various activists become more lively: all this leads to an increase in the number of attacks.

In addition, the size of the DDoS market is inversely proportional to that of the cryptocurrency market, which we've written about several times. This is because DDoS and mining capacities are partially interchangeable, so botnet owners tend to deploy them in mining when cryptocurrency prices are high and in DDoS when they fall. We witnessed precisely that in Q4, and not for the first time: a rise in the number of DDoS attacks amid a sharp drop in the value of cryptocurrencies.

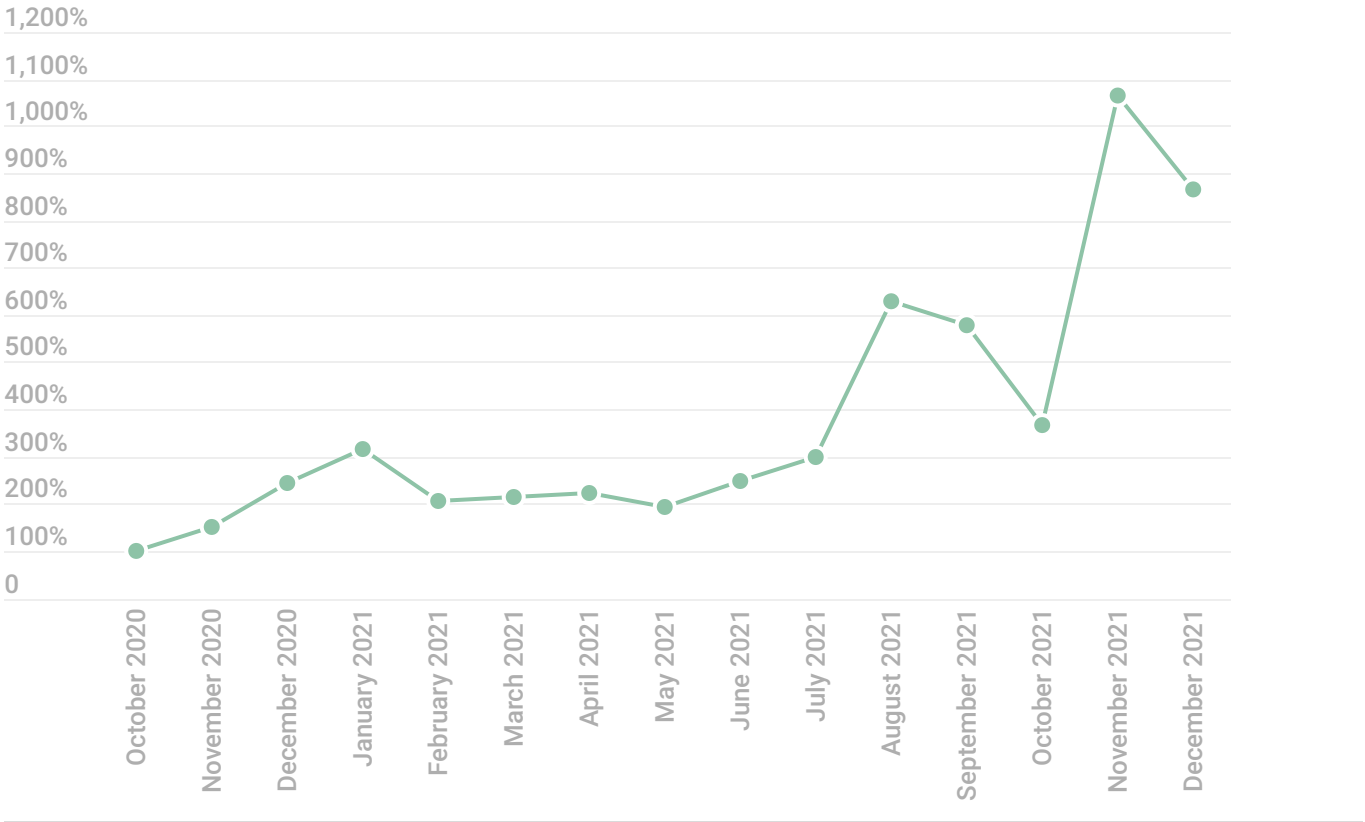
Both of these factors — seasonal fluctuations and falling cryptocurrency prices — buoyed the DDoS attack market throughout Q4, hence the 1.5-fold increase. This becomes even clearer when viewing the stats by month: October accounted for 16% of all DDoS attacks in Q4, November 46% and December 38%.



Percentage distribution of DDoS attacks by month, Q4 2021 (download)

Now let's see where the frightening 4.5-fold increase relative to the previous year came from. In contrast to 2021's all-time high Q4, 2020 posted a record low. In Q4 2020, we observed the opposite situation: a declining DDoS market against the backdrop of rampant cryptocurrency prices. In fact, the DDoS market spent just about the whole of 2021 recovering from this collapse, hence such impressive growth: in essence, 2021's all-time high divided by 2020's all-time low.

The diagram below clearly shows the increase in the number of DDoS attacks over the year, as well as peaks attributable to the cryptocurrency collapse in the summer of 2021 and at the end of the year.



Dynamics of DDoS attacks, October 2020–December 2021; October 2020 data is taken as 100% (download)

As for DDoS targets, the cross-industry distribution of attacks was fairly even — we cannot say that DDoS activity was higher in any particular sector. Perhaps the only thing of note was the spike in attacks on educational resources in November (largely in the Moscow region) and December (largely in the Republic of Tatarstan). We cannot pinpoint the reason for this, but most likely the attacks were related to regional specifics in the field of education, for example, the exam or vacation schedule.

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 Q4 2021.

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. 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

Most of all, attackers in Q4 took aim at US-based resources: the country accounts for 43.55% of attacks and 44.54% of unique targets.

Our DDoS Intelligence system recorded 86,710 DDoS attacks.

The quarter's quietest days fell on Chinese Singles' Day and Black Friday, two mega shopping events.

94,29% of attacks lasted less than 4 hours.

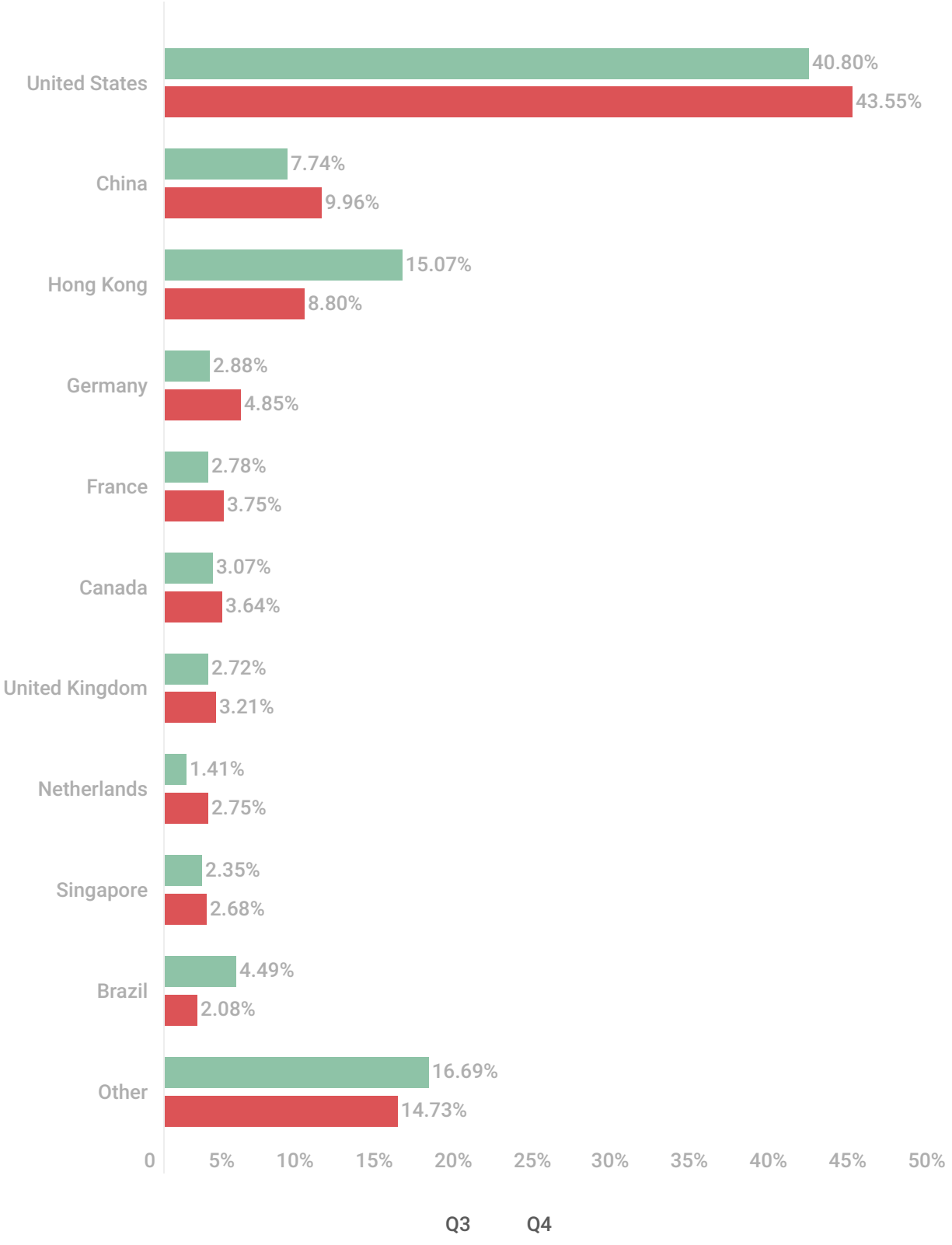
Half of the DDoS attacks were carried out by means of UDP flooding.

46,49% of the botnet C2 servers were located in the US.

70,96% of attacks on Kaspersky SSH honeypots were carried out by bots in Russia.

DDoS attacks geography

In Q4, as in previous quarters in 2021, the bulk of DDoS attacks targeted US-based resources (43.55%). And the country's share in the geographic distribution rose once more. China (9.96%) returned to second place, up 2.22 p.p. on the previous reporting period, while the Hong Kong SAR (8.80%) took bronze: its share fell by a factor of more than 1.5 against the previous quarter.

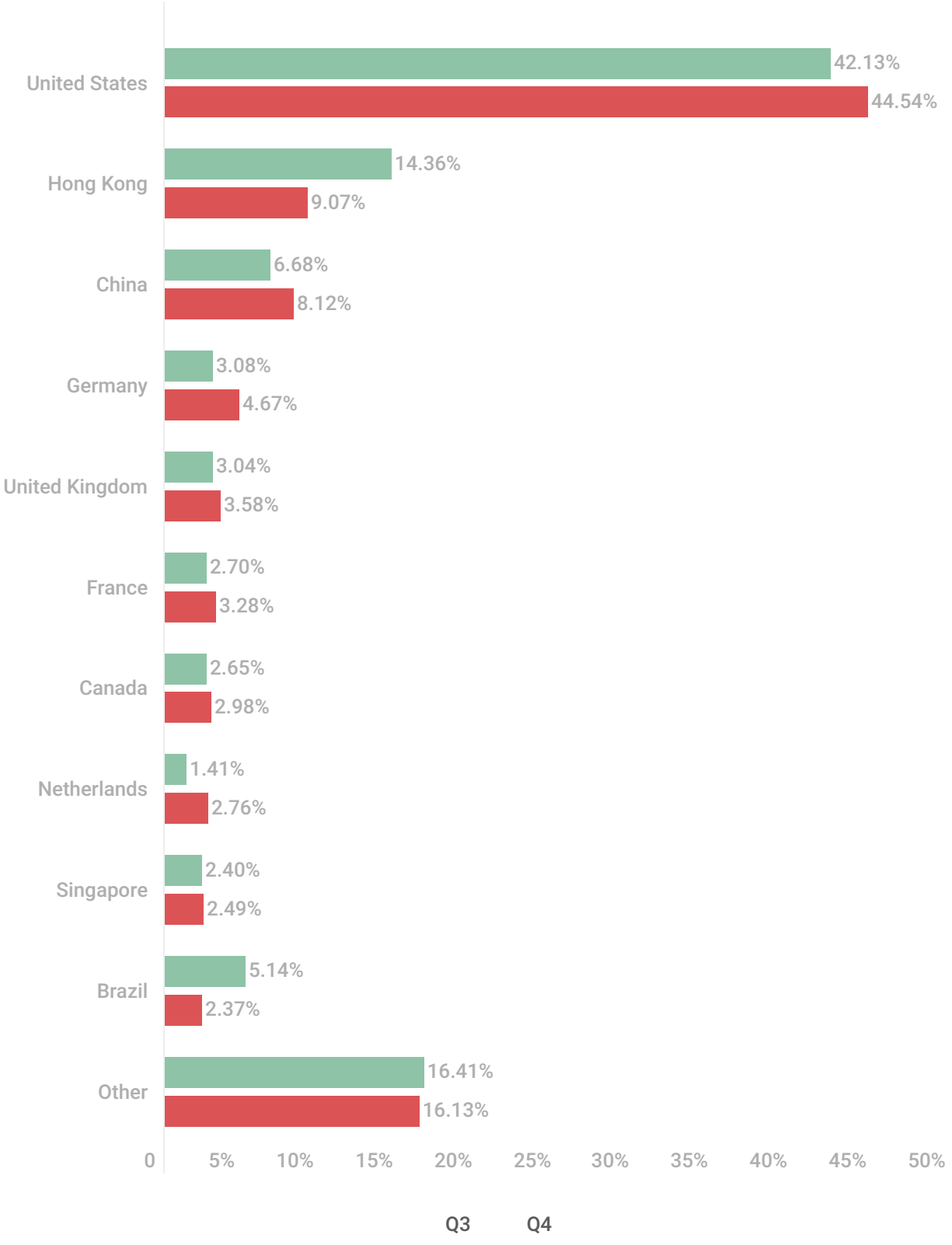


kaspersky

Distribution of DDoS attacks by country and territory, Q3 and Q4 2021 (download)

The share of attacks increased in Germany (4.85%) and France (3.75%), which moved up to fourth and fifth positions, respectively. Canada (3.64%) remained in sixth place, the UK (3.21%) climbed to seventh, while eighth spot in Q4 went to the Netherlands (2.75%), where things had been relatively calm in the previous reporting period. Rounding out the TOP 10 countries and territories by number of attacks at the end of 2021 are Singapore (2.68%) and Brazil (2.08%), whose share more than halved from the previous quarter.

As usual, the geography of unique targets mirrored the distribution of individual attacks. The most targets were located in the US (44.54%), whose share increased compared to the previous quarter. The second and third lines are taken by the Hong Kong SAR (9.07%) and China (8.12%), respectively.



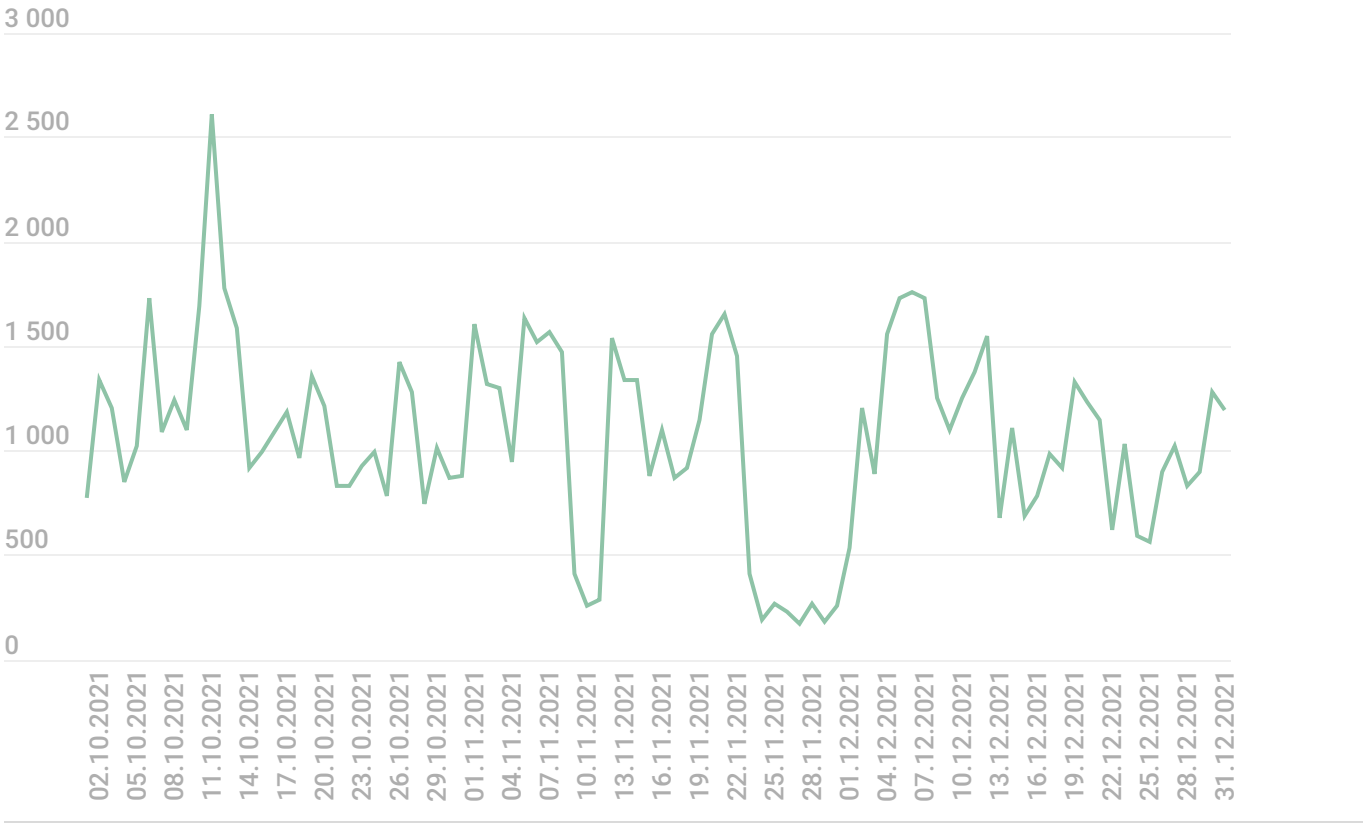
kaspersky

Distribution of unique targets by country and territory, Q3 and Q4 2021 (download)

In fourth place by number of targets is Germany (4.67%), followed in fifth by the UK (3.58%). Next come France (3.28%) and Canada (2.98%). The share of these four countries increased slightly in Q4, and they moved up one rank from Q3. Eighth by number of unique targets was the Netherlands (2.76%), whose share almost doubled, and rounding out the TOP 10, as in the ranking by number of attacks, were Singapore (2.49%) and Brazil (2.37%), whose share almost halved.

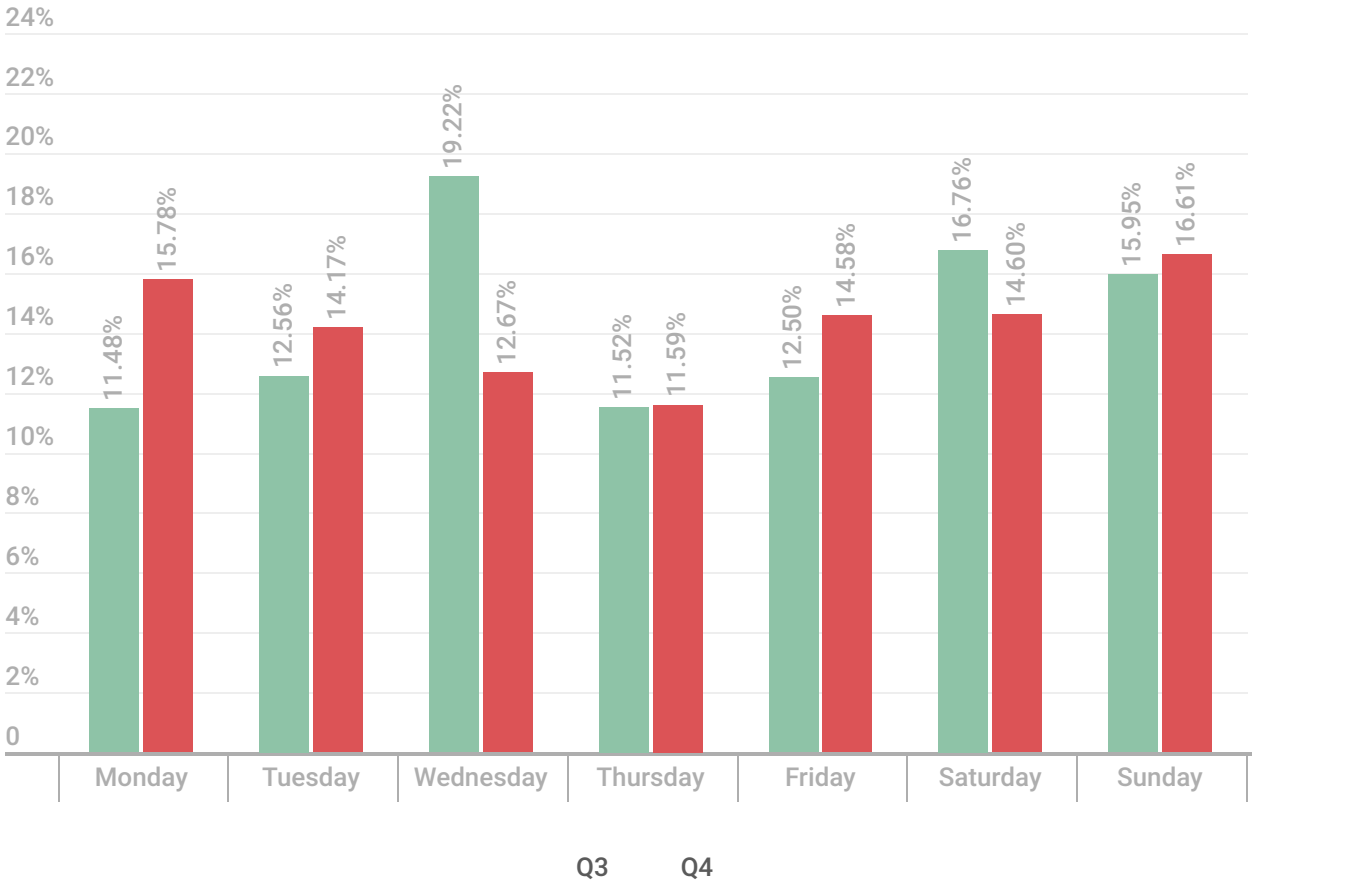
Dynamics of the number of DDoS attacks

During Q4, our DDoS Intelligence system recorded 86,710 DDoS attacks on resources worldwide. In contrast to the previous reporting period, which saw several unusually stormy days, the attacks were distributed relatively evenly throughout the quarter: from 500 to 1,500 per day. However, we did see a surge in DDoS activity on October 11, with 2,606 attacks in 24 hours. November, meanwhile, was marked by two notable drops in DDoS activity: on November 9–11 and 23–30, the number of attacks fell below 500 per day. Curiously, the first drop came on Chinese Singles' Day and the second on Black Friday. Both dates are associated with massive online sales, which tend to cause a spike in various kinds of web attacks.



Dynamics of the number of DDoS attacks, Q4 2021 (download)

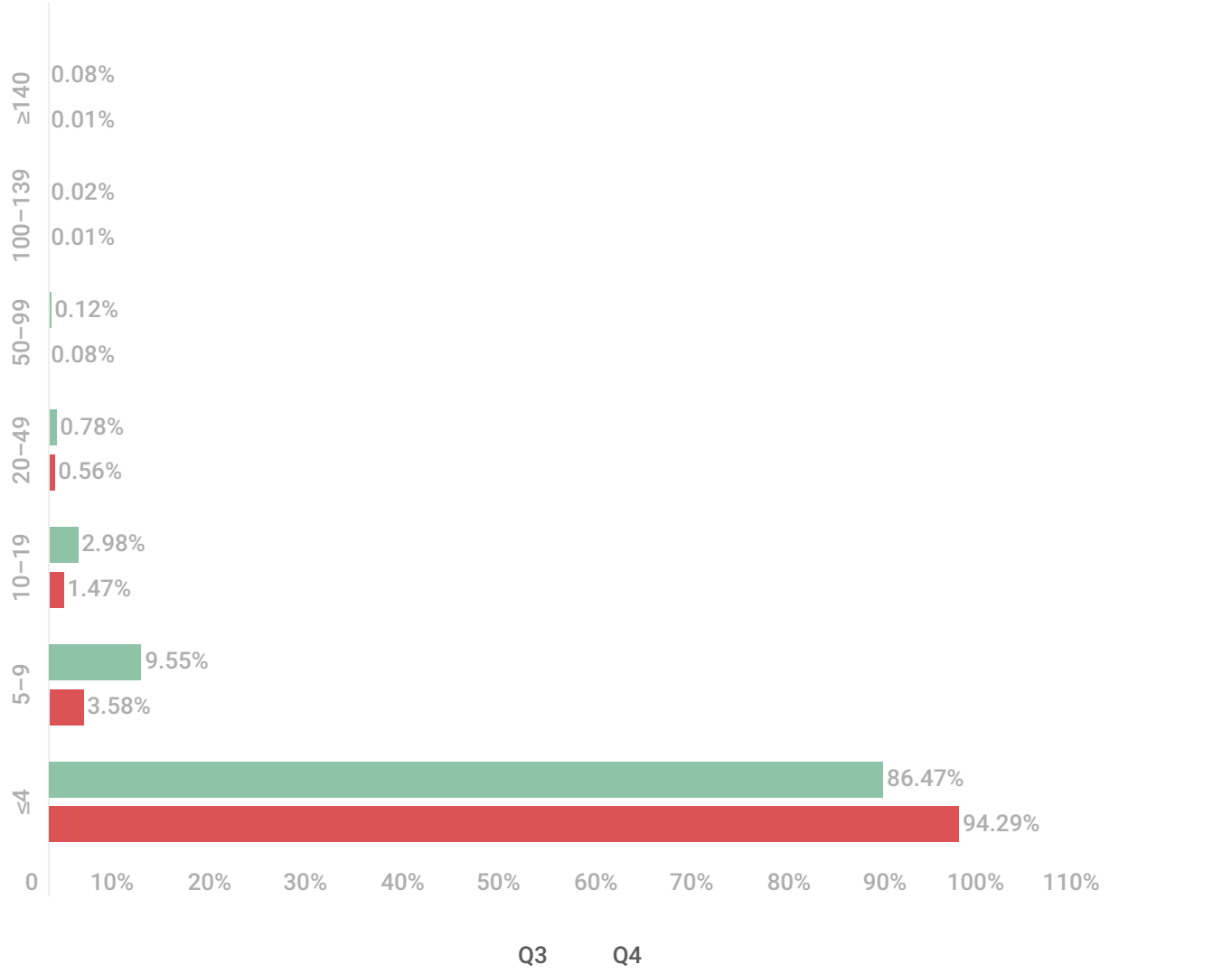
As we noted above, Q4 lacked the dramatic bursts of DDoS activity seen in its predecessor. This was reflected also in the distribution of attacks by day of the week: the spread between the most and least active days was 5.02%, down 2.72 p.p. on Q3. We observed the most DDoS attacks on Sundays (16.61%) — this day's share in the distribution of attacks climbed by 0.66 p.p.; Thursday (11.59%) remained the quietest day, despite its share increasing slightly. The shares of Monday (15.78%), Tuesday (14.17%) and Friday (14.58%) also increased, while those of Wednesday (12.67%) and Saturday (14.60%) decreased, with Wednesday in Q4 being the second calmest day after Thursday.



Distribution of DDoS attacks by day of the week, Q3 and Q4 2021 (download)

Duration and types of DDoS attacks

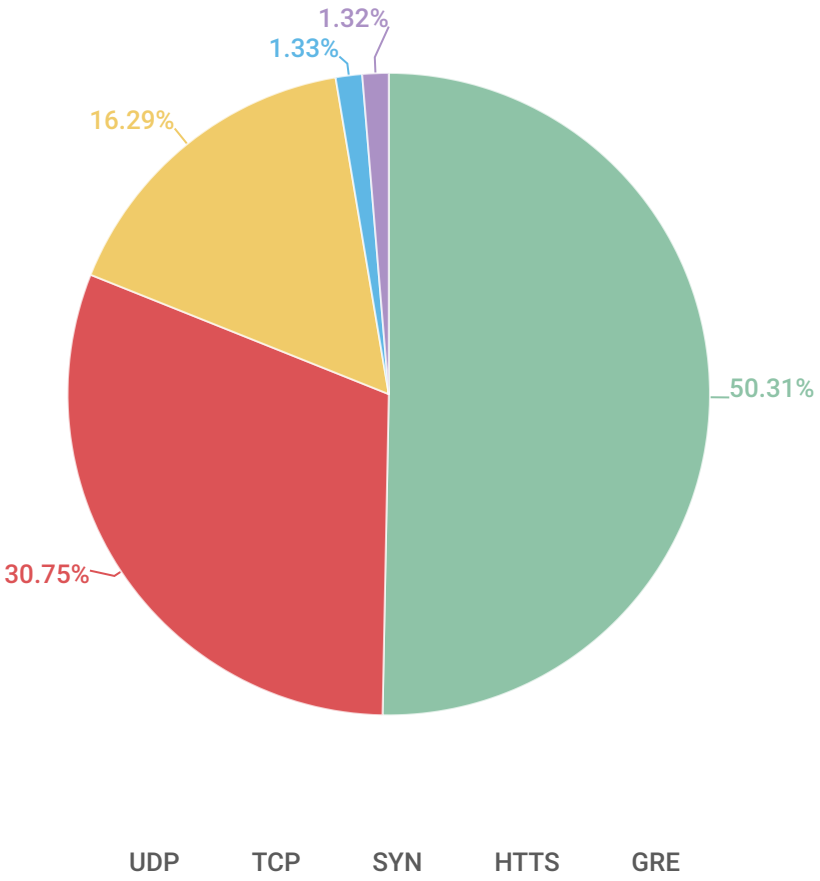
In Q4, we observed an increase in the share of very short (less than 4 hours) DDoS attacks, which accounted for 94.29% of the total, plus a significant drop in the number of long ones: only 0.02% of attacks lasted more than 100 hours. What's more, the longest attack in the quarter was one-third shorter than the longest in the previous reporting period — 218 hours, or just over nine days. Consequently, the average DDoS attack duration fell once more, this time to just under two hours.



kaspersky

Distribution of DDoS attacks by duration, Q3 and Q4 2021 (download)

In terms of attack types, in Q4 we again saw a redistribution of forces. UDP flooding came out on top again, with more than half of all attacks deploying this method. The share of TCP flooding (30.75%) also increased markedly, while that of SYN flooding (16.29%) decreased more than three times. HTTP (1.33%) and GRE flooding (1.32%) stayed put, although their shares increased slightly.

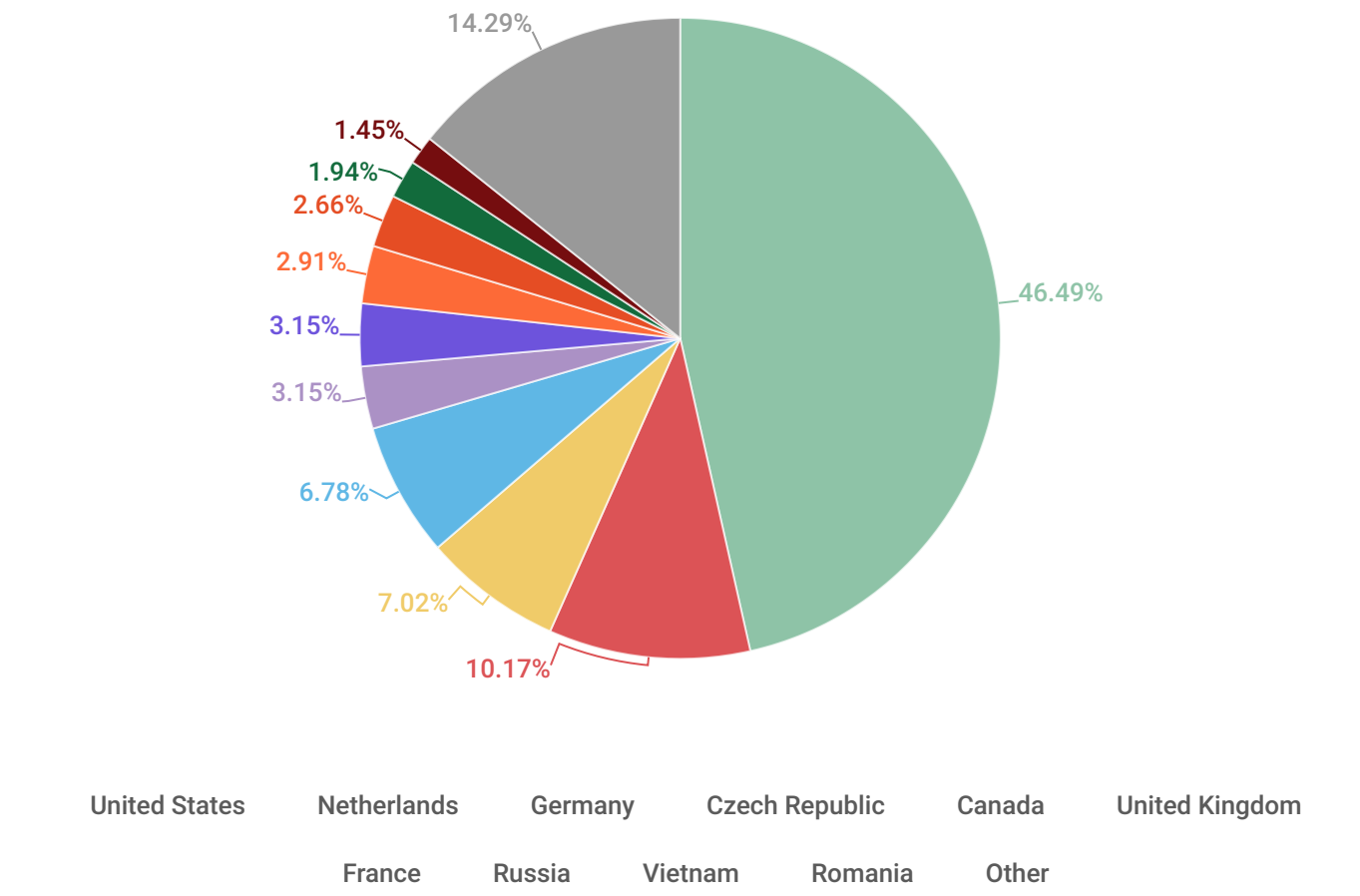


kaspersky

Distribution of DDoS attacks by type, Q4 2021 (download)

Geographic distribution of botnets

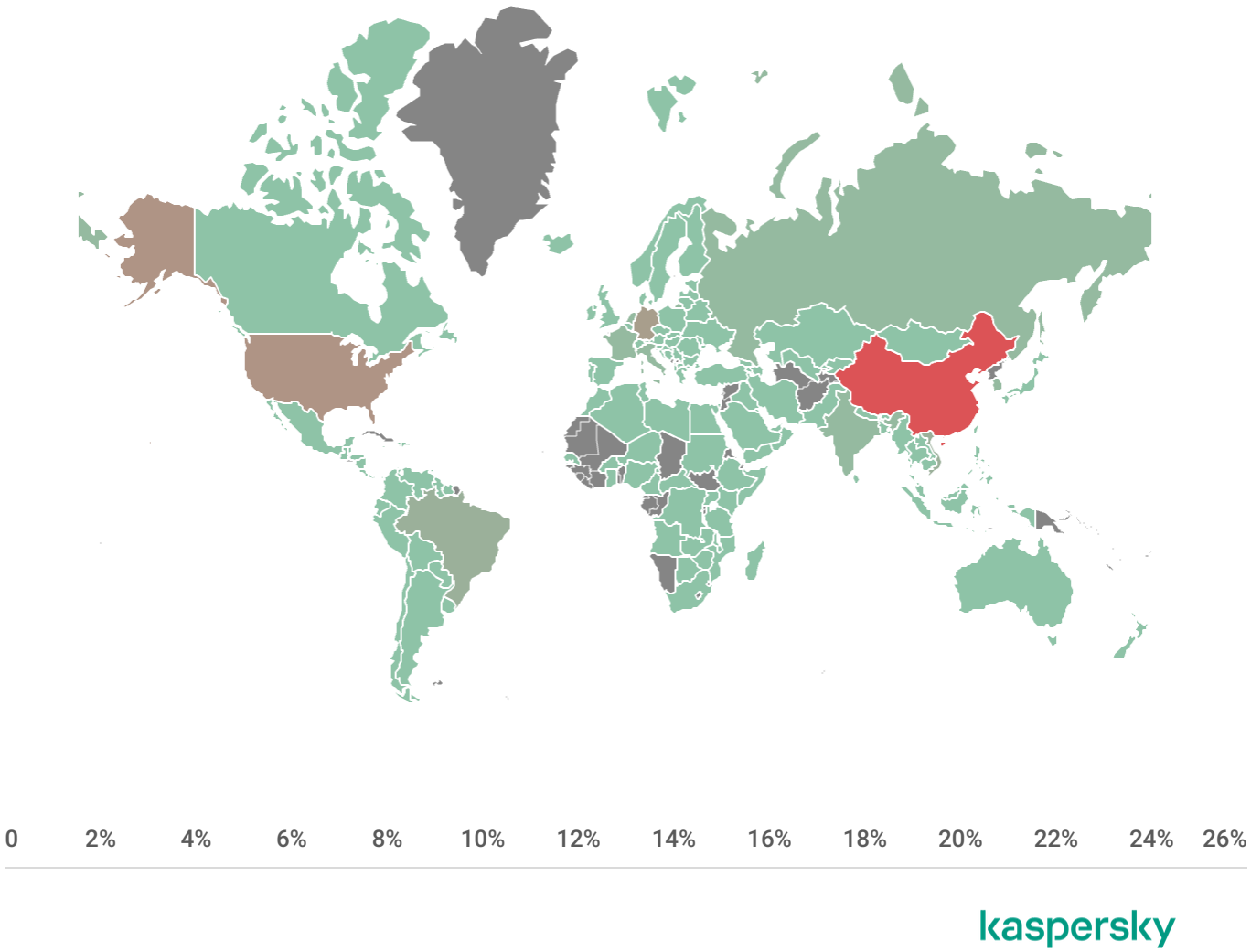
The most botnet C2 servers active in Q4 were located in the US (46.49%), whose share increased by 3.05 p.p. against the previous reporting period. The Netherlands (10.17%) and Germany (7.02%) swapped places. A further 6.78% of C2 servers were located in the Czech Republic, whose share grew almost by 3 p.p., while Canada and the UK each had a 3.15% slice. France hosted 2.91% of the active botnet infrastructure, while 2.66% of C2 servers operated out of Russia. Also in the TOP 10 countries by location of botnets were Vietnam (1.94%) and Romania (1.45%).



Distribution of botnet C2 servers by country, Q4 2021 (download)

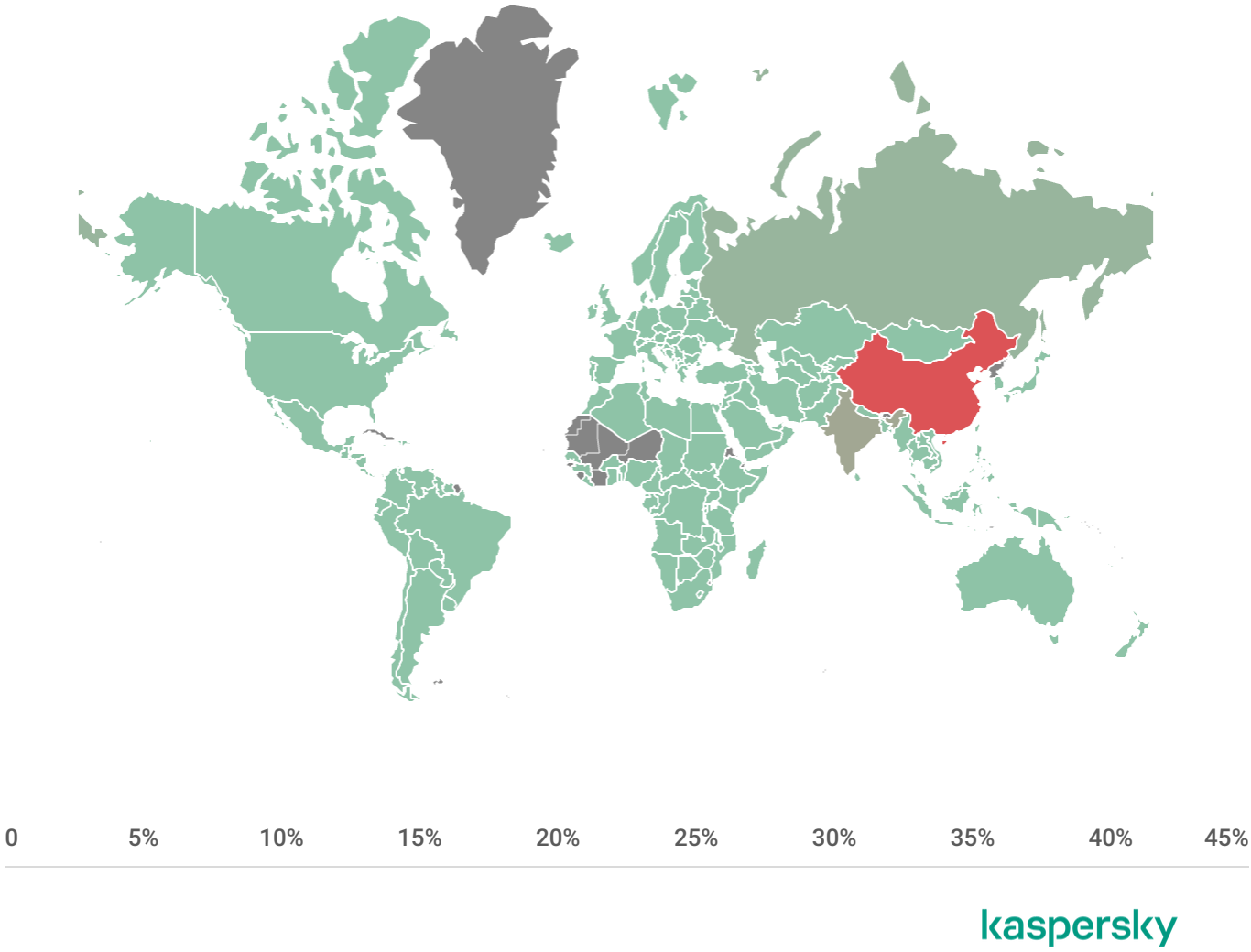
Attacks on IoT honeypots

As for bots attempting to expand botnets in Q4, the largest share of devices that attacked Kaspersky SSH honeypots were located in China (26.73%), the US (11.20%) and Germany (9.05%). At the same time, the share of the first two countries decreased, while the latter added 3.47 p.p. against Q3. Another 5.34% of active bots were located in Vietnam, and 5.13% in Brazil. That said, the vast majority of attacks on our honeypots (70.96%) originated in Russia, where only 2.75% of attacking devices were located; while Vietnam accounted for just 7.94% of attacks, and the US 4.84%. This most likely means that at least one Russian bot showed a high level of performance.



Geographic distribution of devices from which attempts were made to attack Kaspersky SSH honeypots, Q4 2021 (download)

Most of the devices that attacked our Telnet traps, as in the previous quarter, were situated in China (44.88%), India (12.82%) and Russia (5.05%). The first country's share increased by 3.76 p.p., while the latter two saw a drop of 2.4 and 0.93 p.p., respectively. The lion's share of attacks on Kaspersky honeypots came from China (65.27%).



Geographic distribution of devices from which attempts were made to attack Kaspersky Telnet honeypots, Q4 2021 (download)

Conclusion

On the one hand, Q4 met our expectations for this period; on the other, it surprised us. For example, instead of the expected increase in DDoS activity during major online sales, we saw a botnet lull. A feature of the quarter was the large number of very short DDoS attacks, as well as a slew of media reports about short but powerful attacks.

Now for our forecasts. Going by previous years' trends, we expect Q1 2022 to produce roughly the same indicators as Q4 2021. But the situation in the world and, in particular, the cryptocurrency market is too volatile to make such a confident prediction. The bitcoin price has fallen to half its peak value, but remains high. It suffered a similar collapse in the middle of last year, but after that grew even stronger. If cryptocurrencies shoot up again, we could see a significant drop in the DDoS attack

market, but if they sink even further, we will probably see an increase. It is impossible to predict which way it will go. But despite the lack of concrete information, we see no preconditions for any major fluctuations, and expect figures similar to those in Q4.

BOTNETS CYBERCRIME DDOS-ATTACKS INTERNET OF THINGS MALWARE MIRAI

Authors

Expert ALEXANDER GUTNIKOV Expert OLEG KUPREEV Expert YAROSLAV SHMELEV