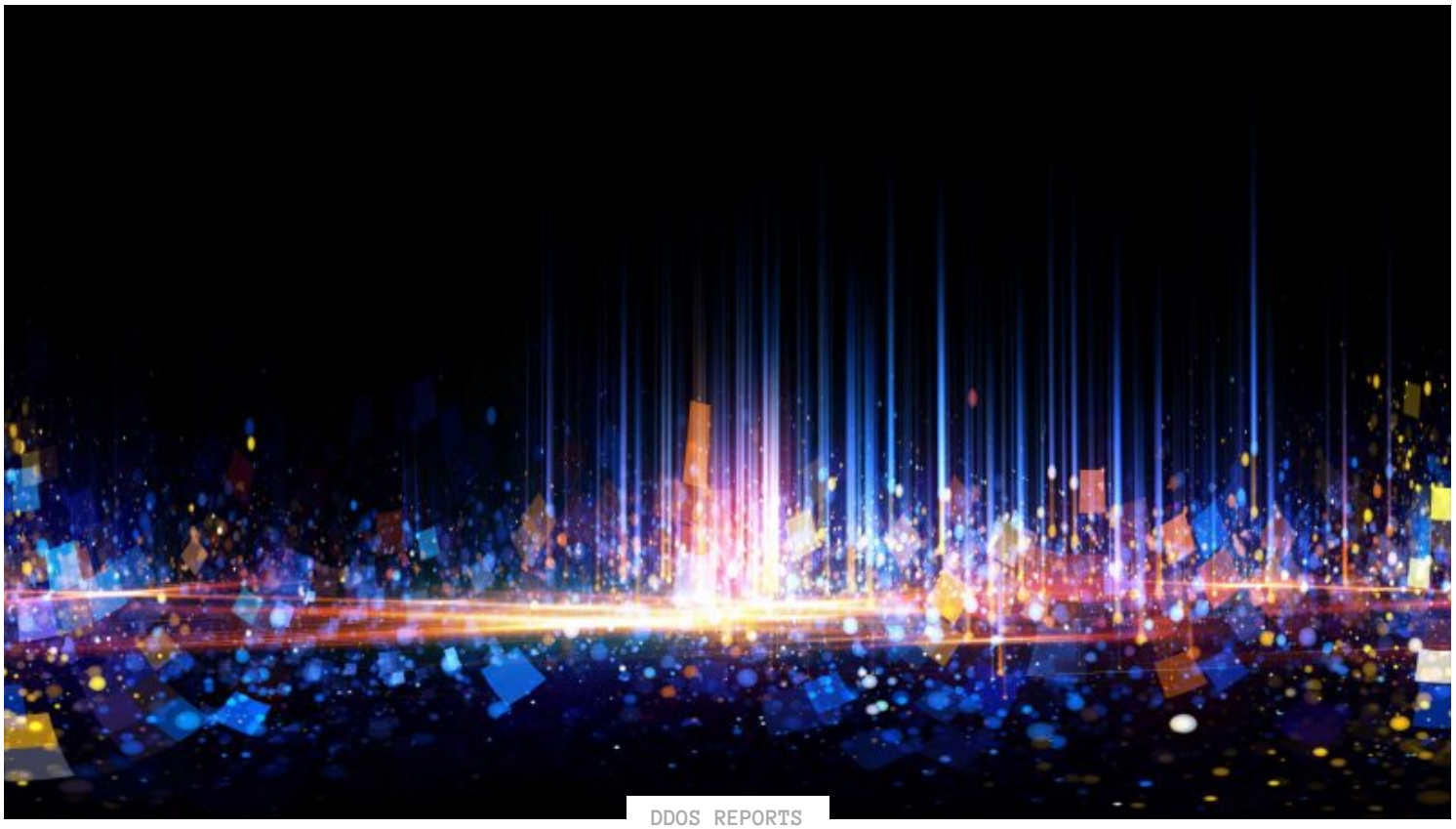


DDOS REPORTS

DDoS attacks in Q2 2021

28 JUL 2021 12 minute read

News overview

In terms of big news, Q2 2021 was relatively calm, but not completely eventless. For example, April saw the active distribution of a new DDoS botnet called Simps — the name under which it introduced itself to owners of infected devices. The malware creators promoted their brainchild on a specially set-up YouTube channel and Discord server, where they discussed DDoS attacks. The actual DDoS functionality of Simps is not original: the code overlaps with the Mirai and Gafgyt botnets.

That said, nor does Gafgyt rely on originality: a handful of modules in the new variants (detected by Uptycs) were all borrowed from Mirai, the most widespread botnet. In particular, Gafgyt's authors copied its implementation of various DDoS methods, such as TCP, UDP and HTTP flooding, as well as its brute-force functionality for hacking IoT devices via the Telnet protocol.

Mirai's code formed the basis of the ZHtrap botnet, which became known this quarter. This malware is of interest for its use of infected devices as honeypots. ZHtrap first collects the IP addresses of devices that attack the trap, and then attempts to attack these devices itself.

Lately cybercriminals have been actively seeking out new services and protocols for amplifying DDoS attacks. Q2 2021 was no exception: in early July researchers at Netscout reported an increase in

attacks using the Session Traversal Utilities for NAT (STUN) protocol. This protocol is used to map internal IP addresses and ports of hosts hidden behind NAT to external ones. Using it, attackers were able to increase the volume of junk traffic by a factor of just 2.32, but in combination with other attack vectors, the DDoS power reached 2TB/s. In addition, hijacking STUN servers to be used as reflectors can disable their main functionality. The organizations that use STUN would be wise to make sure their servers are protected against such attacks. At the time of posting, there were more than 75,000 vulnerable servers worldwide.

Another new DDoS vector has yet to be harnessed by cybercriminals. It is linked to a vulnerability in DNS resolvers that allows amplification attacks on authoritative DNS servers. The bug was named TsuNAME. It works as follows: if a configuration error causes the DNS records of certain domains to point to each other, the resolver will endlessly forward the request from one domain to another, significantly increasing the load on their DNS servers. Such errors can occur by accident: in early 2020, two misconfigured domains caused a 50% increase in the traffic flow on authoritative DNS servers in the NZ domain zone, and a similar incident in a European domain zone led to a tenfold rise in traffic. If an attacker were to create multiple domains pointing to each other, the scale of the problem would be considerably greater.

Attacks on DNS servers are dangerous because all the resources they serve become unavailable, regardless of their size and level of DDoS protection. This is well illustrated by the attack on DNS provider Dyn that downed more than 80 major websites and online services in 2016. To prevent the TsuNAME vulnerability from having the same devastating consequences, the researchers recommend owners of authoritative servers to regularly identify and fix such configuration errors in their domain zone, and owners of DNS resolvers to ensure detection and caching of looped requests.

It was a DNS flood in early April that disrupted the operation of Xbox Live, Microsoft Teams, OneDrive and other Microsoft cloud services. Although the Azure DNS service, which handles the domain names of most of the services, has mechanisms to protect against junk traffic, an unnamed coding error meant it could not cope with the flow of requests. The situation was aggravated by legitimate users trying in vain to access the unresponsive services. However, Microsoft fixed the bug fairly quickly, and the services were soon up and running again.

One other large-scale DDoS attack swept through Belgium, hitting Belnet and other ISPs. Users across the country experienced service interruptions, and websites in the BE domain zone were temporarily unavailable. Junk traffic was sent from IP addresses in 29 countries worldwide, and, as Belnet noted, the attackers kept changing tactics, making the attack extremely difficult to stop. It forced the Belgian parliament to postpone several sessions, while educational institutions had problems with distance learning, and the transport company STIB likewise with the sale of tickets. Online registration systems for COVID-19 vaccinations were also affected.

The council of Grenoble-Alpes Métropole in France also had to suspend a session for several hours. A DDoS attack involving about 60,000 bots made it impossible to broadcast the event live.

Besides Belnet, several other European ISPs were targeted by DDoS attacks. For example, Ireland's Nova fell victim to cybervillains. No confidential data was affected, a spokesperson said, adding that "we are the latest Irish ISP to be attacked and we won't be the last, as the criminals cycle through Irish networks one by one."

That said, there is no need to direct junk traffic at ISPs' own resources in order to disrupt their networks. For instance, Zzoomm, a British broadband provider, suffered from a DDoS assault on one of its upstream suppliers, which in turn was not the real target: cybercriminals were trying to extort a ransom from one of its customers.

In general, DDoS ransomware attacks continued to gain momentum. A cybercriminal group known for its fondness of masquerading as various APT outfits again made the news, this time under the fictitious moniker Fancy Lazarus, composed of the names of two groups: Lazarus and Fancy Bear. Although cybercriminals attack organizations the world over, the victims of Fancy Lazarus were predominantly in the US, and the size of the ransom was lowered from 10–20 to 2 BTC.

Avaddon ransomware operators also tried to intimidate victims through DDoS attacks. In early May, they flooded the site of Australian company Schepisi Communications with junk traffic. The organization partners Telstra, a major Australian provider, selling SIM cards and cloud services on the latter's behalf. Later that same month, French insurance company AXA, one of the largest in the field, also fell victim to Avaddon. As in the case of Schepisi Communications, besides encrypting and stealing data from several of its branches, the cybercriminals carried out a DDoS attack on its websites. After a string of devastating attacks in June, the ransomware creators announced its retirement.

In May, the Irish Health Service Executive (HSE) was hit by DDoS. The attacks would have been unremarkable had they not been immediately followed by an invasion of Conti ransomware. Whether these events are related is uncertain, but the ransomwarers could have used DDoS as a cover to penetrate the company's network and steal data.

Attacks on educational institutions continued in Q2, occurring as they do throughout the school year. For example, malicious actors forced Agawam Public Schools in Massachusetts to shut down their guest network to protect the main network. This meant that Internet access was available only on school-issued devices.

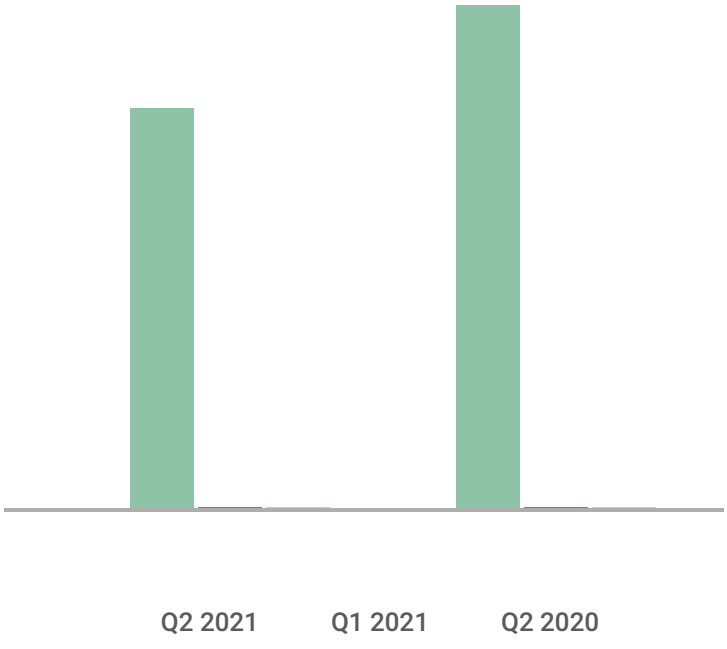
Nor did video games escape attention this reporting period. The *Titanfall* and *Titanfall 2* servers suffered DDoS-related outages in April and May. At least some of these attacks may have targeted specific streamers. To protect against attackers, enthusiasts created a mod that hides players' names. However, this did not stop the attacks on the game servers. As for the developer, Respawn

Entertainment, it took care of DDoS protection, but not in *Titanfall*, rather in *Apex Legends*, where the new version, in the event of an attack, chucks everyone out of the game, with compensation for any losses incurred. Back in *Titanfall*, however, the problem is so acute that a hacktivist player decided to hack *Apex Legends* to raise awareness of it.

Another hacktivist, after a decade of hiding from the law, was caught in Mexico and deported to the US. Christopher Doyon had been one of the organizers of the 2010 protests against a law banning rough sleeping in Santa Cruz, California. Following the crackdown on the protests, Doyon launched a DDoS attack on the Santa Cruz County website. Having been charged, the hacktivist failed to appear at a court hearing pending trial in 2012. Consequently, he was put on the international wanted list. Now Doyon will finally stand trial on the decade-old charges.

Quarter trends

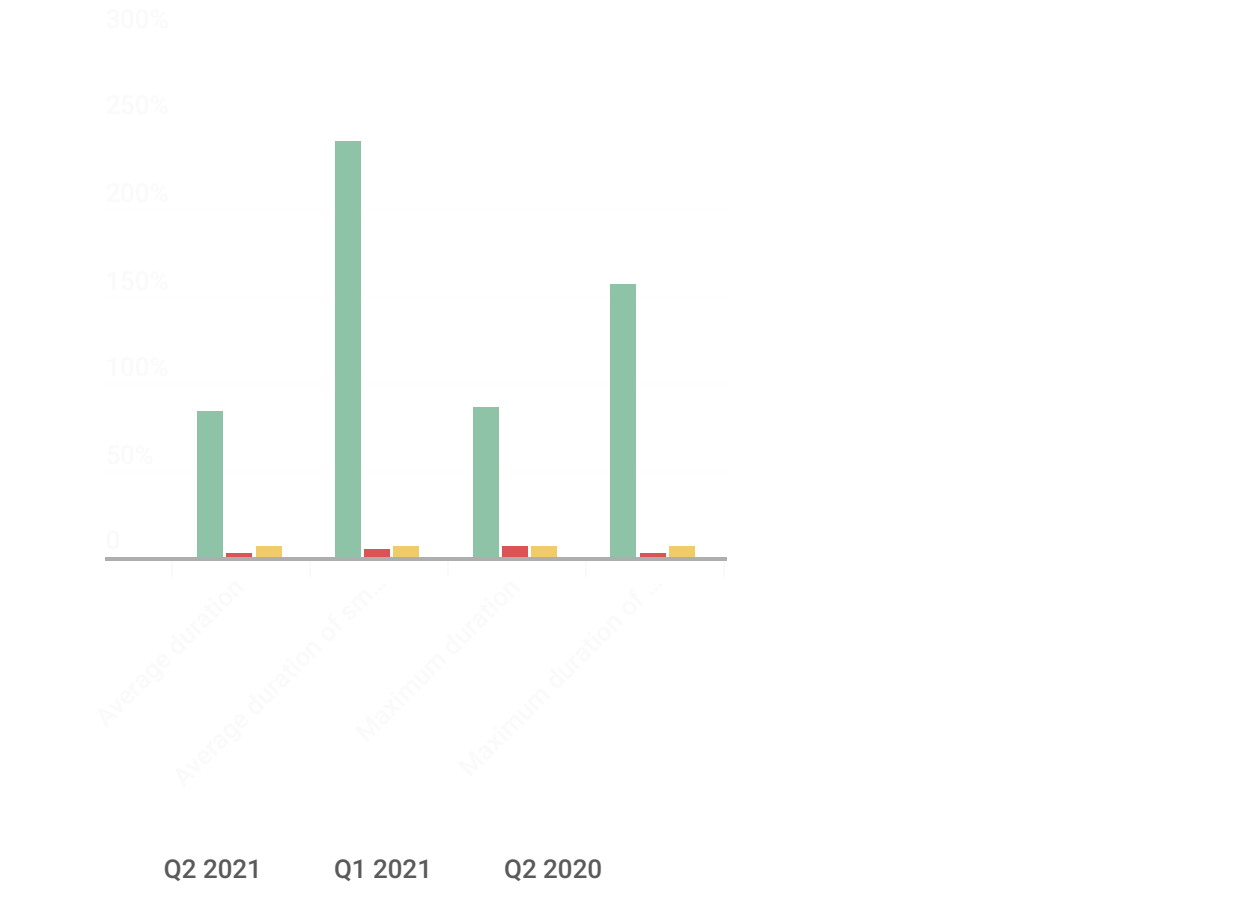
As expected, Q2 2021 was calm. We recorded a slight fall in the total number of DDoS attacks compared to the previous quarter, which is typical for this period and seen every year, barring the anomalous 2020. This drop we traditionally associate with the start of the vacation period. It tends to continue through Q3, and we expect no change this year.



kaspersky

Comparative number of DDoS attacks, Q1 and Q2 2021, and Q2 2020. Q2 2020 data is taken as 100% (download)

Note the exceptional duration of smart DDoS attacks in the past quarter. This is due to several abnormally long, though not too powerful, attacks on law enforcement resources. We see no correlation between these attacks and any high-profile event. There may be a causal connection somewhere, but since there is no way of knowing, it remains to interpret them as statistical anomalies, which do crop up every so often. With these attacks excluded from the sample, the data on DDoS duration is closer to the norm with different periods fluctuating by no more than 30% relative to each other.



kaspersky

DDoS attack duration, Q1 and Q2 2021, and Q2 2020. Q2 2020 data is taken as 100% (download)

Statistics

Methodology

Kaspersky has a long history of combating cyber threats, including DDoS attacks of all types and complexity. The company experts monitor botnets using the Kaspersky DDoS Intelligence system.

As part of the Kaspersky DDoS Protection solution, DDoS Intelligence intercepts and analyzes commands sent to bots from C&C 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 Q2 2021.

In the context of this report, an 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 web resource was attacked by the same botnet with an interval of 24 hours or more, this is considered as two attacks. Bot requests originating from different botnets but directed at one resource also count as separate attacks.

The geographical locations of DDoS victims and C&C servers are determined by their 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

Q2's leader by number of DDoS attacks is again the US (36%). The share of China (10.28%) continued to fall, while Poland (6.34%) climbed into the TOP 3 most attacked countries.

The most DDoS-active day in the quarter was June 2, when we registered 1,164 attacks. On the quietest day, we observed only 60 DDoS attacks.

Most DDoS attacks occurred on Tuesdays (15.31%), while the calmest day of the week was Sunday (13.26%).

The longest DDoS attack lasted 776 hours (more than 32 days).

UDP flooding was used in 60% of DDoS attacks.

The country with the most botnet C&C servers was the US (47.95%), while the bulk of bots attacking IoT devices in order to assimilate them were located in China.

DDoS attack geography

In Q2 2021, as in Q1, most DDoS attacks were directed at US-based resources (36%). China (10.28%), the perennial leader until this year, continued to lose ground, shedding another 6.36 p.p. Third place this quarter was taken by a newcomer in the ranking, Poland (6.34%), whose share was up by 4.33 p.p. against the previous reporting period. Canada (5.23%), which rounded out the TOP 3 in Q1, fell to fifth place, despite gaining 0.29 p.p.

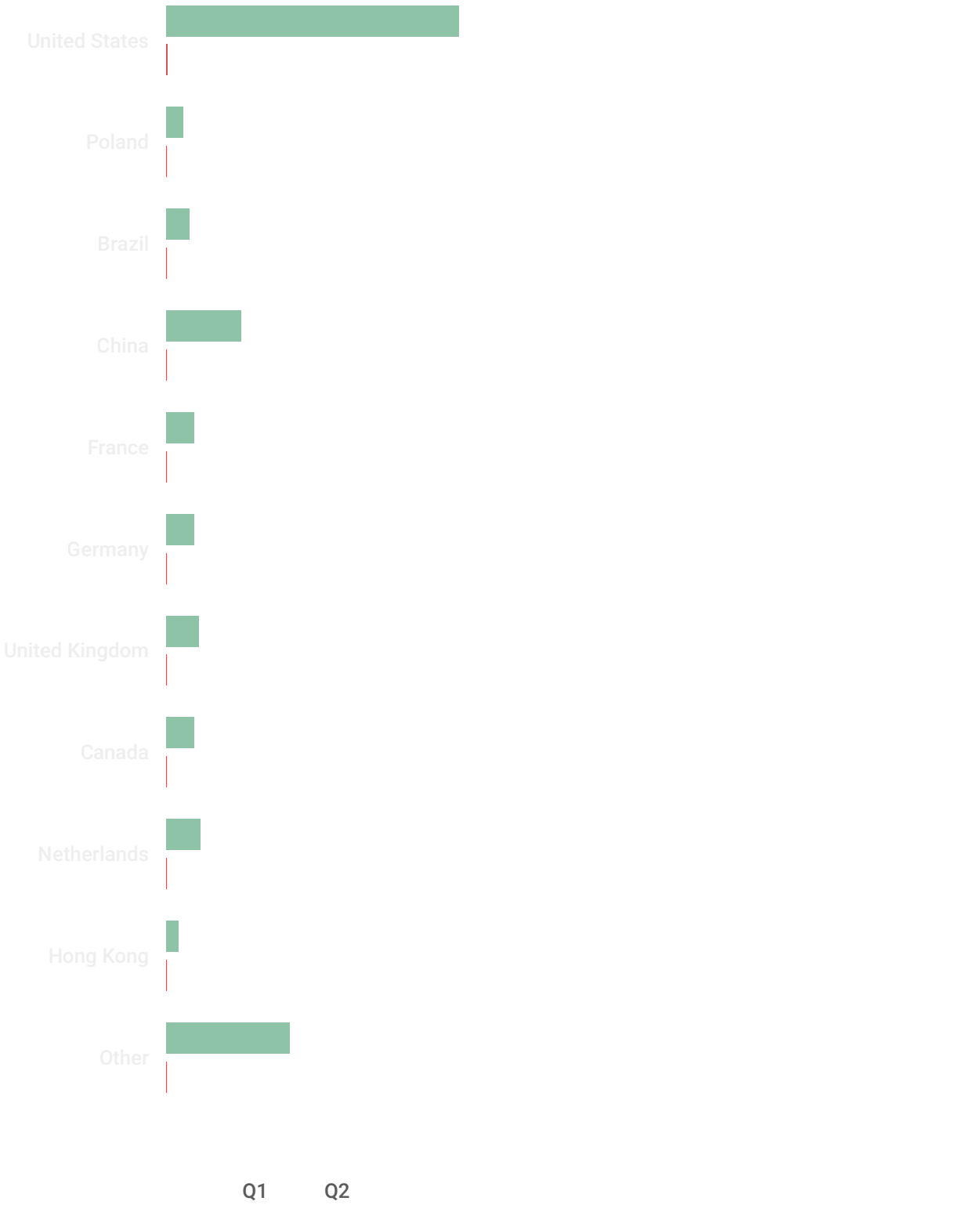
In fourth place by number of DDoS attacks in Q2 was Brazil (6.06%), whose share almost doubled. Sixth in the ranking was France (5.23%), behind Canada by a fraction of a fraction. Germany (4.55%)

remained in seventh position, while the UK (3.82%) moved into eighth. At the foot of the ranking are the Netherlands (3.33%) and Hong Kong (2.46%), whose shares, like China's, continued to nosedive.

kaspersky

Distribution of DDoS attacks by country, Q1 and Q2 2021 (download)

A look at the countries with the highest number of unique targets also shows an increase in DDoS activity in Poland (7.44%) and Brazil (6.25%), which ranked second and third, respectively, and a decrease in activity in China (5.99%), which dropped to fourth place. The TOP 10 tends to be pegged to the list of countries with the highest number of DDoS attacks: the US remains in top spot (38.60%), fifth to eighth places belong to France (4.97%), Germany (4.86%), the UK (4.40%) and Canada (4.20%), respectively, followed by the Netherlands (3.40%) and Hong Kong (1.81%).



kaspersky

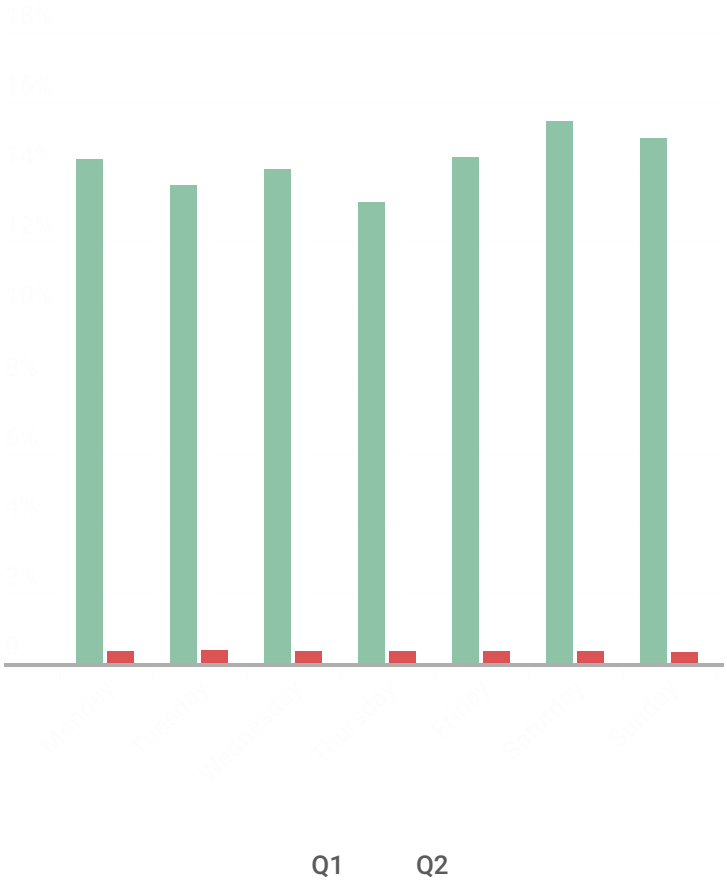
Distribution of unique DDoS targets by country, Q1 and Q2 2021 (download)

Dynamics of the number of DDoS attacks

As noted above, Q2 turned out relatively calm. On average, the number of DDoS attacks per day fluctuated between 500 and 800. On the quietest day of the reporting period, April 18, we observed only 60 attacks. On two other days, June 24 and 25, the number of attacks fell short of 200. Nevertheless, Q2 had its share of turbulent days with more than 1,000 DDoS attacks. For instance, we observed 1,061 attacks on April 13 and 1,164 on June 2.

Dynamics of the number of DDoS attacks, Q2 2021 (download)

The distribution of DDoS attacks by day of the week in Q2 was, if anything, even more uniform than in Q1: the difference between the busiest and quietest days was only 2.05 p.p. At the same time, activity shifted to the start of the week. The share of Monday through Thursday relative to Q1 increased, while the end of the week, having been the most turbulent in the previous reporting period, grew calmer. We observed the highest number of attacks on Tuesdays (15.31%), while the quietest day this time was Sunday (13.26%).



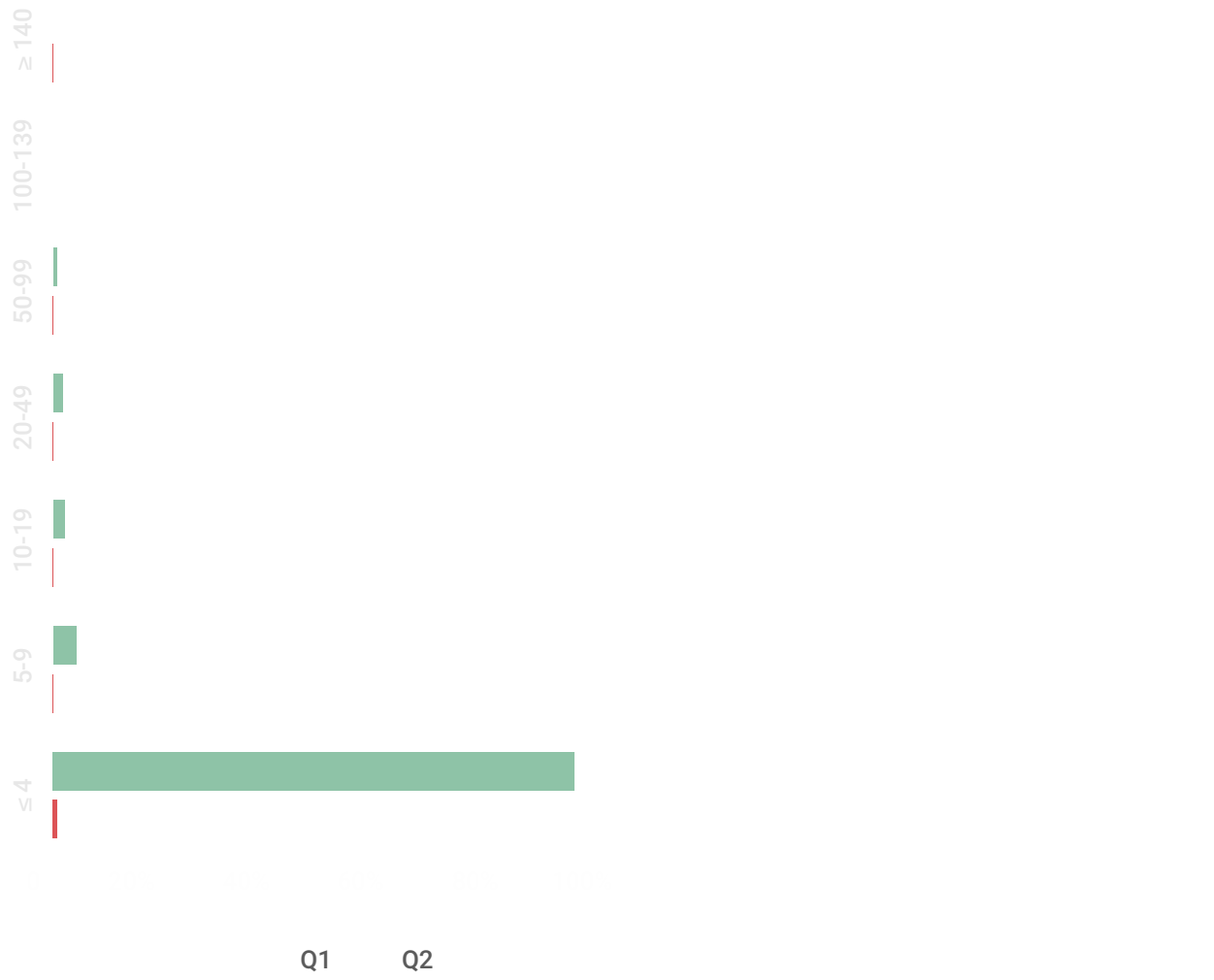
kaspersky

Distribution of DDoS attacks by day of the week, Q1 and Q2 2021 (download)

Duration and types of DDoS attacks

In Q2, the average DDoS attack duration remained virtually unchanged from the previous reporting period: 3.18 hours versus 3.01 in Q1. What's more, there was a slight increase both in the share of very short attacks lasting less than 4 hours (from 91.37% to 93.99%) and in the share of long (from 0.07% to 0.13%) and ultra-long (from 0.13% to 0.26%) ones. By contrast, the share of moderately long attacks in Q2 fell slightly, and attacks lasting 5–9 hours (2.65%) lost 1.51 p.p.

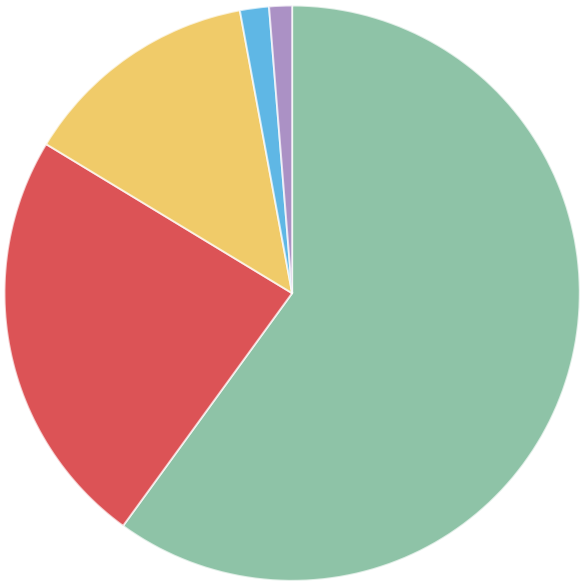
The maximum attack duration continued to increase. If in Q4 2020 we saw no attacks lasting more than 302 hours, the longest attack in Q1 2021 was 746 hours (more than 31 days), and Q2 topped that with a 776-hour-long attack (more than 32 days).



kaspersky

Distribution of DDoS attacks by duration, Q1 and Q2 2021 (download)

Looking at the distribution by type of attack, we see that UDP flooding in Q2 significantly increased its slice (60% vs 42% in Q1). SYN flooding (23.67%), which until 2021 was the most common type of DDoS, is fighting to regain lost territory: this quarter it swapped places with TCP flooding (13.42%) to claim second place.

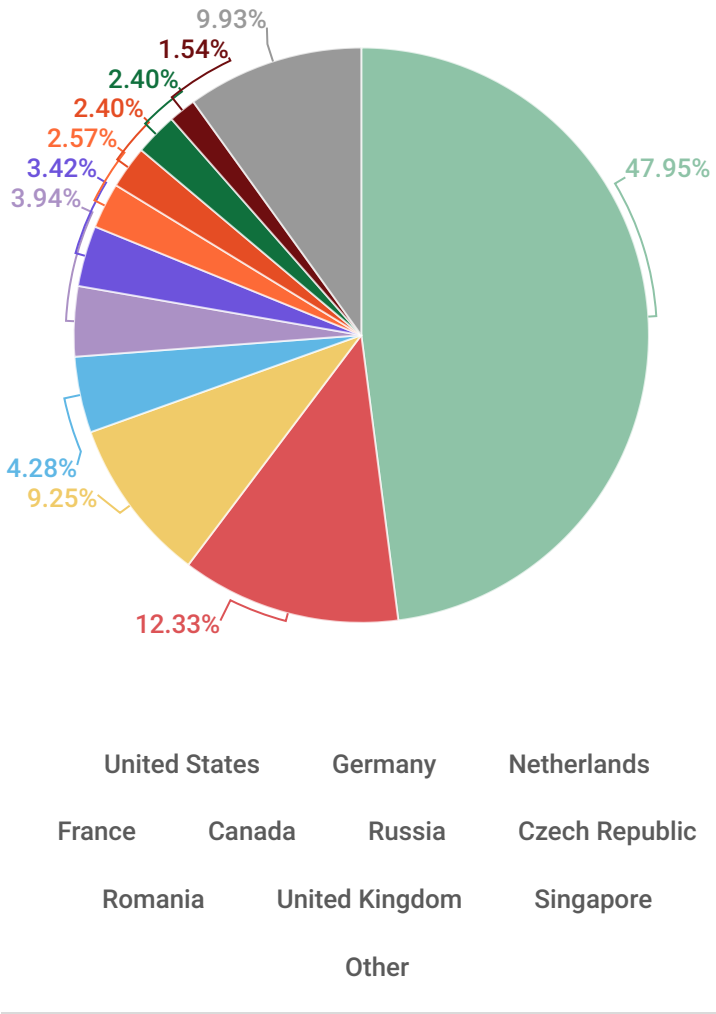


Distribution of DDoS attacks by type, Q2 2021 (download)

Botnet distribution geography

Among botnet C&C servers, 90% were located in ten countries in Q2. The biggest share was in the US (47.95%), which added 6.64 p.p. to its score in the previous reporting period. In second place, as in Q1, is Germany (12.33%), and in third place the Netherlands (9.25%). France (4.28%) retained fourth position, followed by Canada (3.94%), whose share has doubled since last quarter.

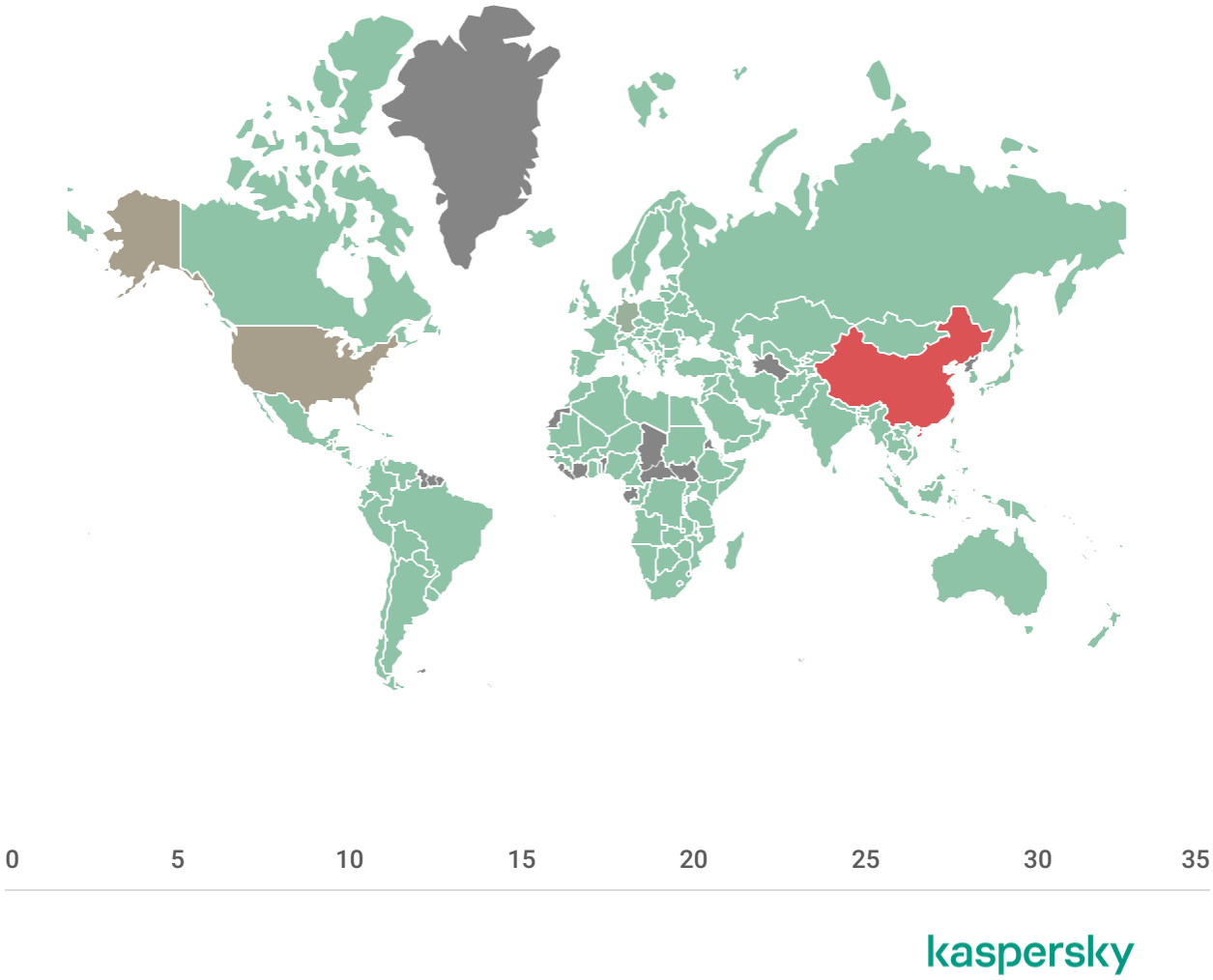
The sixth-placed country by number of botnet C&C servers, as in Q1, is Russia (3.42%). The Czech Republic (2.57%) climbed to seventh place, overtaking Romania (2.40%), which shared eighth and ninth places with the UK (2.40%). Singapore (1.54%) props up the TOP 10, while the Seychelles dropped out of the ranking, having almost no C&C servers used by active botnets.



Distribution of botnet C&C servers by country, Q2 2021 (download)

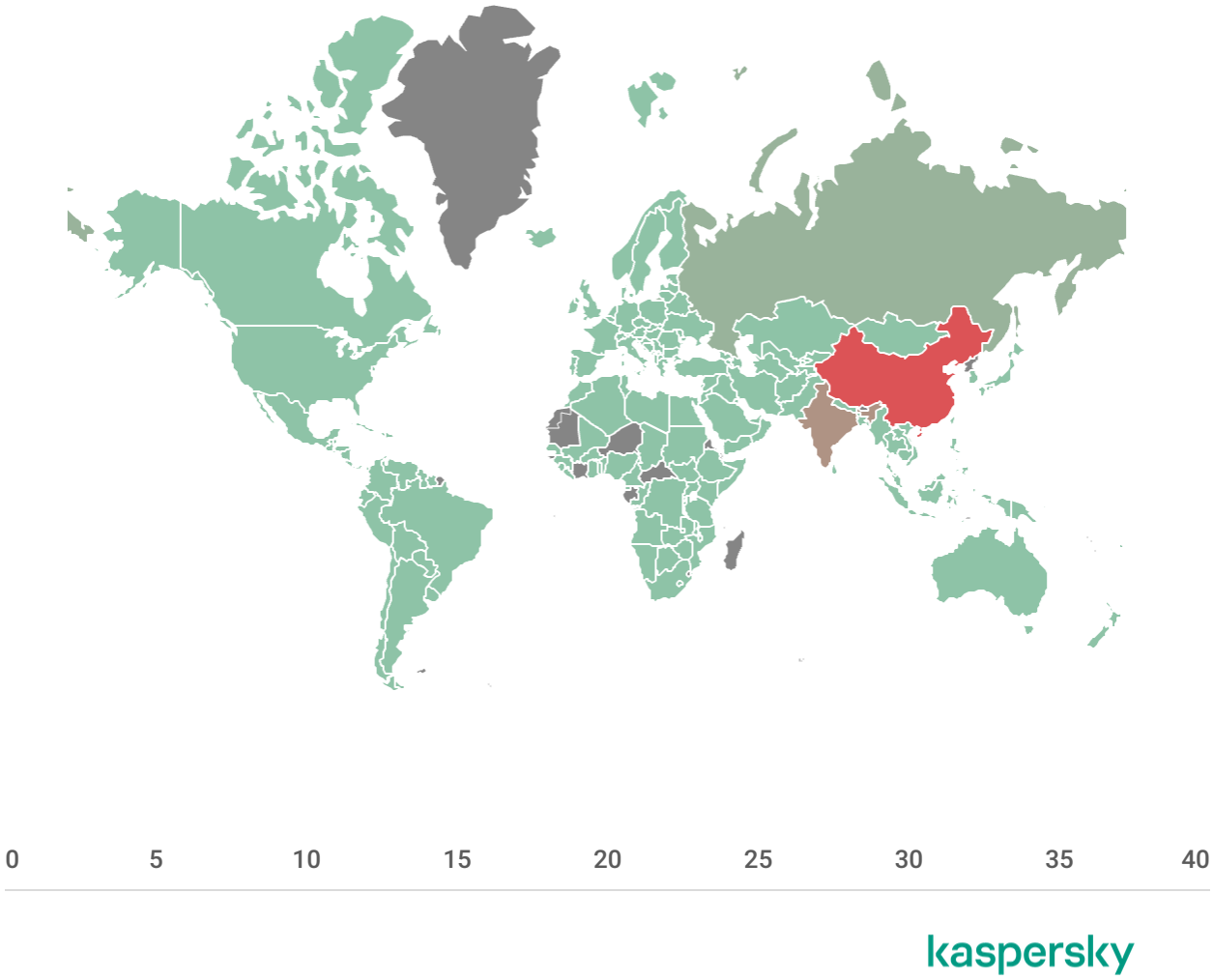
Attacks on IoT honeypots

Also in Q2 2021 we analyzed in which countries bots and servers were attacking IoT devices with a view to botnet expansion. This involved studying the statistics on Telnet and SSH attacks on our IoT honeypots. The country with the most devices from which SSH attacks were launched this quarter was China (31.79%). In second place was the US (12.50%), and in third Germany (5.94%). However, the bulk of attacks via SSH originated in Ireland (70.14%) and Panama (15.81%), which both had relatively few bots. This could suggest that among the attacking devices located in these countries there were powerful servers capable of infecting multiple devices worldwide simultaneously.



Geography of devices from which attempts were made to attack Kaspersky SSH traps, Q2 2021 (download)

The biggest share of bots attacking Telnet traps in Q2 also belonged to China (39.60%). In addition, many bots were located in India (18.54%), Russia (5.76%) and Brazil (3.81%). The attacks originated mostly in these same countries, the only difference being that bot activity in Russia (11.25%) and Brazil (8.21%) was higher than in India (7.24%), while China (56.83%) accounted for more than half of all attacks on Telnet honeypots.



Geography of devices from which attempts were made to attack Kaspersky Telnet honeypots, Q2 2021 (download)

Conclusion

The DDoS market continues to stabilize after last year's shakeup. As expected, Q2 2021 demonstrated the traditional summer lull. That said, we did see some abnormally long attacks, as well as shifts in the DDoS geography. The number of attacks in China, which long topped the ranking, continued to decline, at the same time as DDoS activity in Poland and Brazil increased markedly. Other than that, it was a pretty ordinary second quarter.

At present, we see no grounds for a sharp rise or fall in the DDoS market in Q3 2021. As before, the market will be heavily dependent on cryptocurrency prices, which have been riding high, despite declining relative to their spring peak: 1 BTC is worth US$30,000–35,000, less than a couple of months

ago, but still a tidy sum. With cryptocurrency prices still attractive, the DDoS market is not expected to grow. Most likely, the summer decline typical of the vacation period will continue through Q3.

BOTNETS CYBERCRIME DDOS-ATTACKS INTERNET OF THINGS MALWARE

Authors

ALEXANDER GUTNIKOV

EKATERINA BADOVSKAYA

OLEG KUPREEV

YAROSLAV SHMELEV