

DDOS REPORTS

DDoS attacks in Q1 2020

06 MAY 2020 ⌛ 12 minute read

News overview

Since the beginning of 2020, due to the COVID-2019 pandemic, life has shifted almost entirely to the Web — people worldwide are now working, studying, shopping, and having fun online like never before. This is reflected in the goals of recent DDoS attacks, with the most targeted resources in Q1 being websites of medical organizations, delivery services, and gaming and educational platforms.

For instance, attackers in mid-March tried to disable the [website of the US Department of Health and Human Services \(HHS\)](#). The purpose of the attack was seemingly to deprive citizens of access to official data about the pandemic and measures taken against it. At the same time, unknown cyber actors spread [misinformation](#) in social networks and via text and e-mail about the introduction of a nationwide quarantine in the US. The attempt failed: the HHS website continued to function, despite the increased load.

The victim of another DDoS attack was the large Paris-based [group of hospitals Assistance Publique-Hôpitaux de Paris](#). Cybercriminals attempted to disable the infrastructure of medical institutions. As a result, remote hospital workers were unable to use programs and corporate e-mail for some time. However, the attackers failed to paralyze the entire organization.

The food delivery services [Lieferando \(Germany\)](#) and [Thuisbezorgd \(Netherlands\)](#) found themselves in a more awkward situation. DDoS attacks on both companies meant that although they could accept orders, they could not process them and had to return customers' money. What's more, the cybercriminals targeting Lieferando demanded 2 BTC (a shade over US\$13,000 at the time of writing) to halt the DDoS.

The German distance-learning platform Mebis was [attacked on the very first remote school day](#). The service, which enables teachers in the federal state of Bavaria to exchange materials, homework, and tests with schoolchildren, was down for several hours.

Online games, whose popularity has soared under quarantine, were hit repeatedly. In particular, attackers flooded the servers of [Battle.net](#) and [Eve Online](#) with junk traffic, the latter facing nine straight days of bombardment. Belarusian company [Wargaming](#) also came under fire: players of World of Tanks, World of Warships, and other titles had problems with server speeds for several days. However skeptical users claimed that the problems had nothing at all to do with cybercriminals.

Australian authorities in late March reported a DDoS attack on the MyGov social services portal, but a couple of hours after the major announcement they were forced to [admit they had made a mistake](#). It turned out that the site could not cope with the influx of perfectly genuine requests from citizens out of work as a result of the pandemic.

Besides DDoS attacks directly or indirectly related to the all-conquering coronavirus, this quarter saw a continuation of politically motivated attacks. In the second half of January, for instance, unknown cyber actors made two attempts to bring down the [websites of government agencies](#) and emergency services in Greece. Among the resources taken temporarily offline were the websites of the prime minister, several ministries, the fire service, and the police. The [Turkish group Anka Neferler Tim](#) claimed responsibility for the first attack, but the Greek authorities are not rushing to any final conclusions, especially since the perpetrators of the second attack have yet to announce themselves.

This year will see the next US presidential election, and the runup to it, as always, is accompanied by DDoS attacks. For example, a [voter registration and information website](#) was hit in early February. The attackers employed the PRSD (pseudorandom subdomain attack) technique to send numerous requests to non-existent subdomains of the site. However, the DDoS attempt failed: the resource was protected against attacks of this kind.

Financial institutions were not spared either. In February, the cryptocurrency exchanges [OKEx](#) and [Bitfinex](#) were subjected to sophisticated DDoS attacks. The first has assured that it handled the incident without detriment to users, while the second was forced offline for an hour. According to Bitfinex management, this was necessary to set up specialized protection. Whether the incidents were just similar or related is not known.

The [BitMEX crypto exchange](#) likewise announced a DDoS attack this quarter — not once but twice. Its access problems coincided with a sharp drop in the value of bitcoin, which prompted a wave of suspicion among customers. Some believe that the [exchange intentionally went offline](#) to prevent a mass sell-off. BitMEX later promised to pay compensation, but only to 156 users who had lost deals in the ETH/USD pair.

As in the previous quarter, ransomware attacks by well-known APT groups made the news. In late February, Australian financial institutions [received e-mails demanding large sums](#) in the cryptocurrency Monero. The attackers introduced themselves as the Silence group, and threatened DDoS attacks for non-payment. Earlier, e-mails with similar threats had been received by companies from Singapore, Turkey, South Africa, and other countries. The ransomers went by the various names of Cozy Bear, Fancy Bear, Anonymous, Carbanak, and Emotet in the hope that victims would google them and be scared into compliance.

Unlike these international ransomware groups, a teenager from Odessa who last year tried to DDoS a company that had refused to cooperate was [caught by police](#) in January 2020. The youngster wanted to force a Ukrainian internet service provider to hand over information about a customer. On being refused, he attempted to disable the company's network. The attack was reported to be quite powerful.

Overall, the past quarter was fairly rich in arrests. In February, Arthur Dam was detained in the US charged with carrying out four DDoS attacks on the website of congressional candidate Bryan Caforio in 2018, taking it offline for a total of 21 hours. The prosecution noted that Dam's wife worked for Caforio's rival Katie Hill, who ultimately won the vote.

Another cybercriminal was [detained in Krasnodar](#) in mid-March for attacking the online store of a company in Cherepovets, Russia. Although he had carefully masked the source of the DDoS attack, cyber police managed to trace him. The individual claimed that he had simply wanted to demonstrate his skills and offer his services to the company to defend against DDoS attacks. However, the idea failed even before his arrest, since he was unable to bring down the site.

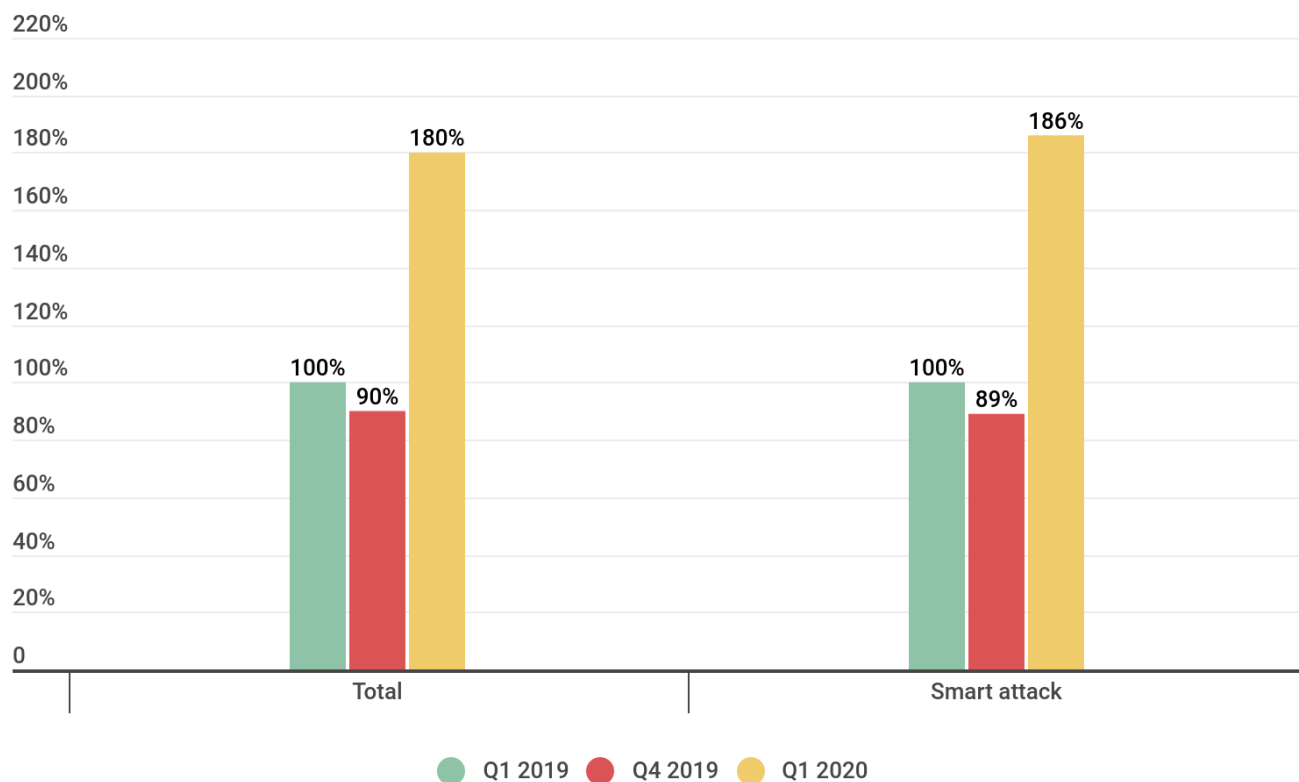
This guy is by no means the only "double agent" in the DDoS world. In New Jersey, [Tucker Preston](#), founder of BackConnect, a DDoS mitigation firm, admitted to a similar crime. From December 2015 to February 2016, Preston hired third parties to bombard the New Jersey-based servers of an unnamed organization with junk traffic. The offense carries up to ten years in jail and a maximum fine of US\$250,000.

The owners of a website allegedly used to launch custom DDoS attacks could also be forced to fork out. Video game publisher [Ubisoft filed a lawsuit](#) against the resource after a string of attacks on the servers of *Tom Clancy's Rainbow Six Siege*. According to the developer, the site — which purportedly

helps clients test their own security — actually specializes in DDoSing games. Ubisoft is seeking the closure of the resource and damages from the owners.

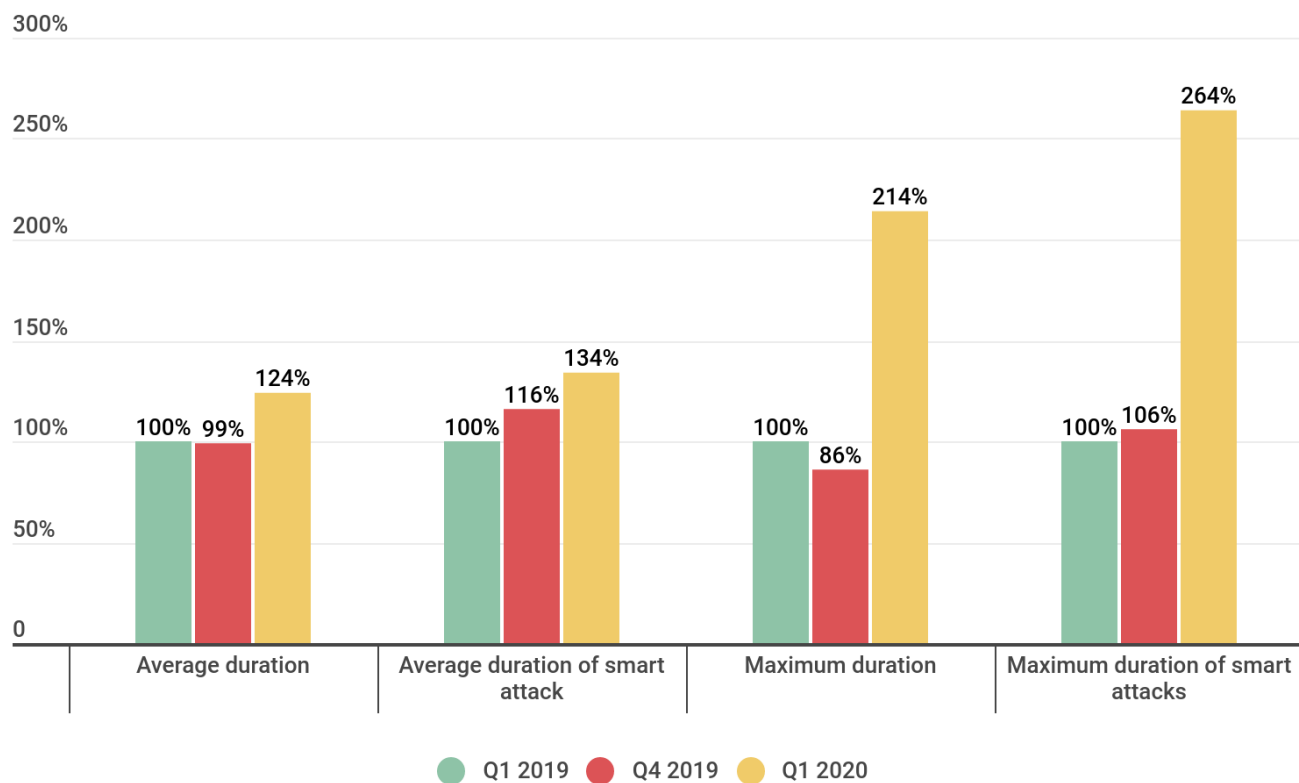
Quarter trends

This quarter has been dominated by the coronavirus pandemic, which has shaken up many things in the world, including the DDoS market. Contrary to our forecast in the last report, in Q1 2020 we observed a significant increase in both the quantity and quality of DDoS attacks. The number of attacks doubled against the previous reporting period, and by 80% against Q1 2019. The attacks also became longer: we observed a clear rise in both the average and maximum duration. The first quarter of every year sees a certain spike in DDoS activity, but we did not expect this kind of surge.



kaspersky

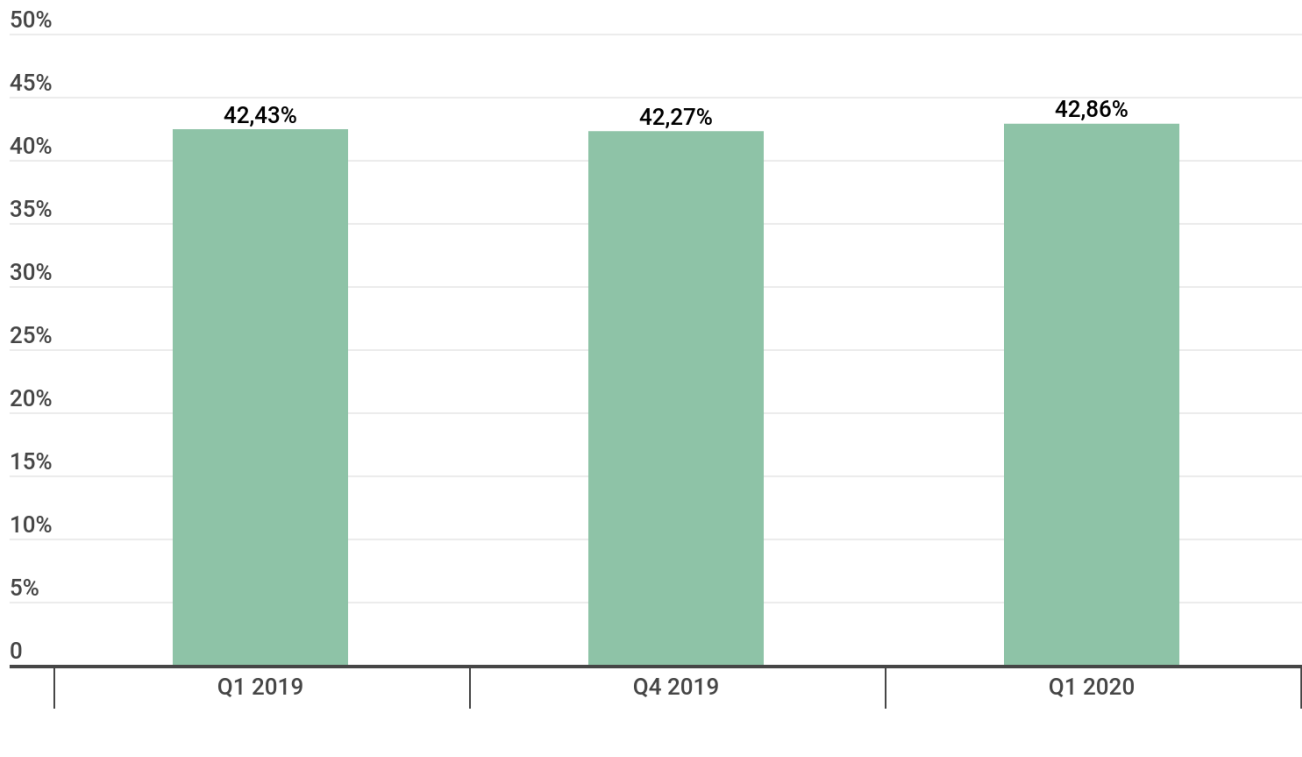
Comparison of the total number of DDoS attacks in Q1 2020 and Q1 and Q4 2019; Q1 2019 is taken as the 100% reference value ([download](#))



kaspersky

Duration of DDoS attacks in Q1 2020 and Q1 and Q4 2019; Q1 2019 is taken as the 100% reference value ([download](#))

Against a backdrop of overall growth, the share of smart attacks remained virtually unchanged over the past year: the first quarters of 2019 and 2020 were at the same level, around 42%. This points to a rise in interest in DDoS attacks on the part of both professionals and amateurs: the number of overall attacks is growing at the same pace as the number of smart attacks, so the proportion has not changed.



kaspersky

***Share of smart attacks in the total number of DDoS attacks in Q1 2020 and Q1 and Q4 2019
([download](#))***

Interestingly, the number of DDoS attacks on educational and administrative web resources tripled compared to the same period in 2019. Moreover, such attacks in Q1 2020 amounted to 19% of the total number of incidents, against just 11% a year ago.

The upswing in cybercriminal interest in such resources could be linked to the spread of COVID-19, which has created more demand for distance-learning services and official sources of information. Since the start of 2020, the pandemic has affected all industries. So it is logical for it to impact the DDoS market too. Going forward, this effect may become even more pronounced.

Although it is difficult to predict anything at a time of such global instability, it can be assumed that the attacks will not decrease: many organizations are now switching to remote working, and with that the set of viable targets is increasing. If earlier the target in most cases was companies' public resources, now key infrastructure elements, such as corporate VPN gateways or non-public web resources (mail, corporate knowledge base, etc.), may be at risk. This is opening up new niches for attack organizers, and could lead to DDoS market growth.

Statistics

Methodology

Kaspersky has a long history of combating cyber threats, including DDoS attacks of all types 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 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 Q1 2020.

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 web resource was attacked by the same botnet with an interval of 24 hours or more, then 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-attack victims and C&C 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 2020, most C&C servers were still registered in the US (39.93%), while most bots were in Brazil.

In terms of the dynamics of the number of attacks overall, this quarter was very similar to the last – with peaks of more than 230 attacks on February 14 and 15 and a drop to 16 attacks on January 25.

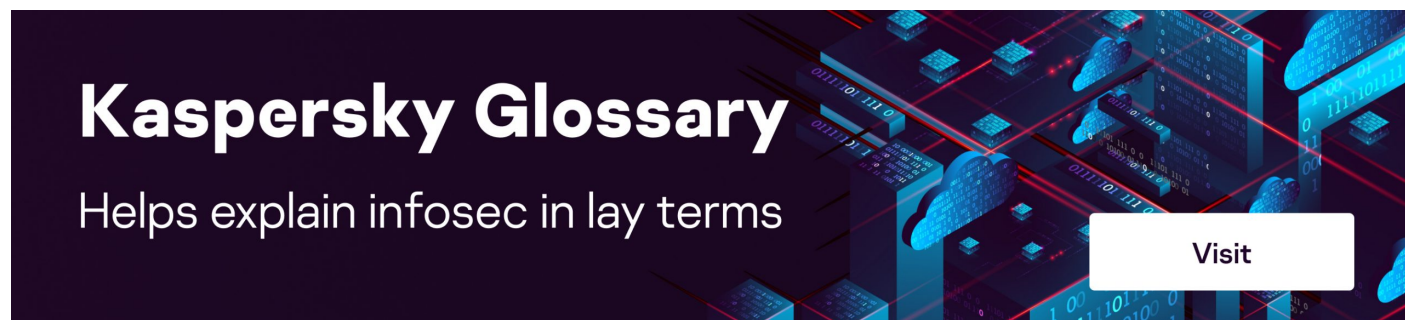
DDoS attackers were most active on Mondays, and more likely to rest on Wednesdays.

SYN flooding is still the most popular type of attack (and even strengthened its position with 92.6% of all attacks), while ICMP attacks unexpectedly jumped ahead of all other varieties into second place.

Windows botnets continue to gain popularity: the share of attacks using them grew by 3 p.p. to 5.64%.

Geography of unique IP addresses used in attacks

This quarter, we decided to look at the distribution by country of botnets and their component bots. To do so, we analyzed the location of the unique IP addresses from which attacks on our [honeypots](#) were registered.

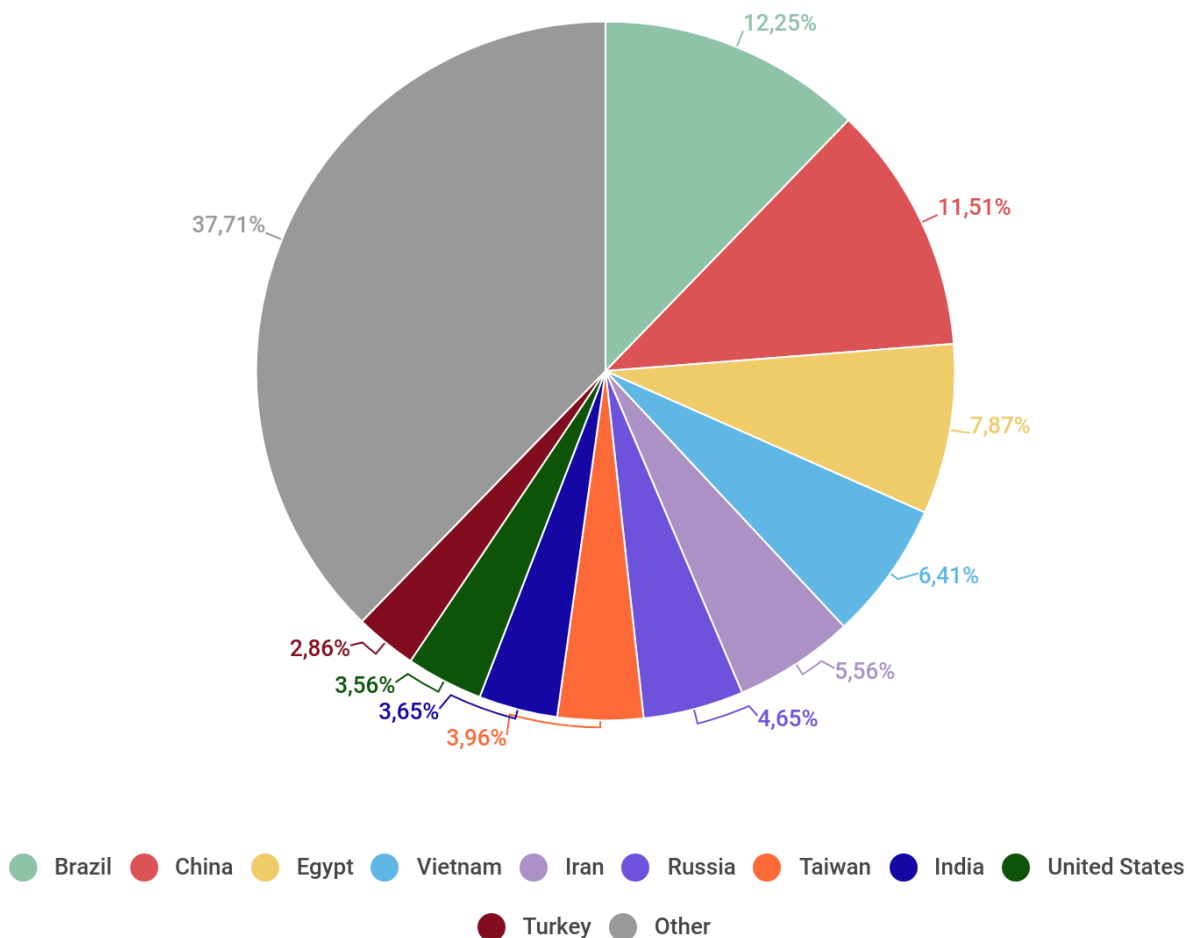


Kaspersky Glossary

Helps explain infosec in lay terms

[Visit](#)

First place in the TOP 10 countries by number of bots goes to Brazil, with 12.25% of unique IP addresses. In second place, less than one percentage point behind, is China (11.51%), while third position — by a much wider margin — is taken by Egypt (7.87%). The remaining TOP 10 countries scored from 6.5% to 2.5% of the total number of bot IP addresses. The rating also featured several Asian countries (Vietnam (6.41%) in fourth; Taiwan (3.96%) in seventh; India (3.65%) in eighth), plus Iran (5.56%) in fifth place, Russia (4.65%) in sixth, and the US (3.56%) in ninth. The TOP 10 is rounded out by Turkey, the source of 2.86% of unique addresses used for attacks.



kaspersky

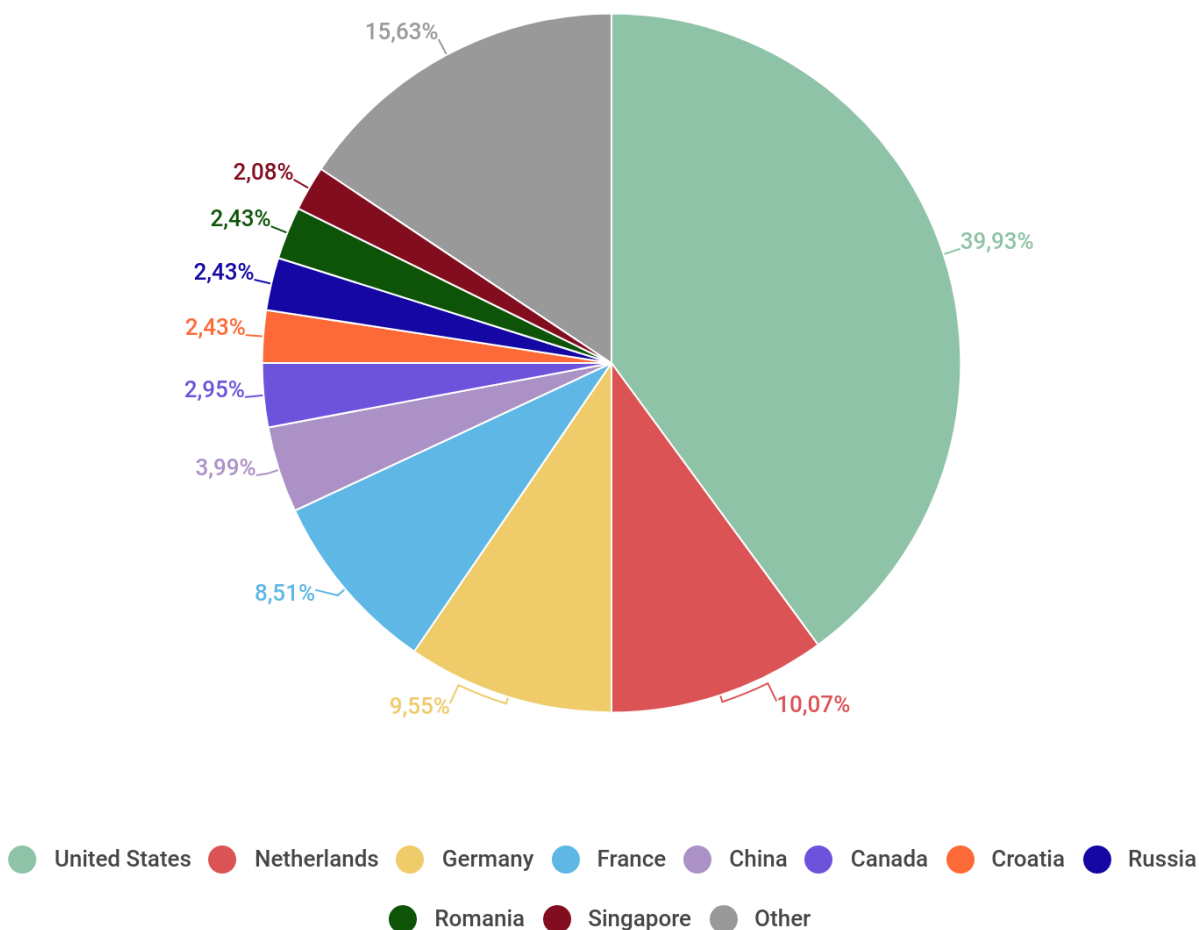
Distribution of botnets by country, Q1 2020 (download)

Curiously, this distribution only partially correlates with the attack statistics. Whereas China has long occupied top spot in the ranking by number of attacks, and Vietnam is a regular visitor to the TOP 10, the leader of the rating by number of unique IPs, Brazil, has only been in the TOP 20 once this past year, taking 20th position in Q1 2019. More often than not, it appears only in the bottom third of the TOP 30, not unlike Iran, which closes off the TOP 5 by number of bots. As for Egypt (3rd place by number of bots), it is the source of very few registered attacks, so it generally lies outside even the TOP 30.

Botnet distribution geography

If individual attack devices are mainly located in South America, Asia, and the Middle East, C&C servers, as in the previous quarter, are more often registered in the US and Europe. First place by number of C&Cs is retained by the US, where in Q1 2020 almost 40% of the total were registered (down 18.5 p.p. against the end of last year). Second place is occupied by the Netherlands (10.07%), which climbed up from eighth, and third goes to Germany (9.55%), which last quarter was nowhere to be seen in the TOP 10. As we saw above, of the TOP 3 countries by number of C&C servers, only the US hosted a significant number of bots.

Fourth position by number of C&Cs went to another European country, this time France (8.51%), climbing two rungs up the ladder. China showed the exact opposite trend, falling from third to fifth (3.99% vs 9.52% in Q4 2019). Canada (2.95%) took sixth place, up from ninth, while seventh position was shared by Russia, Romania (back in the TOP 10 after a quarterly break), and newcomer Croatia. Each of these countries scored 2.43% of the total number of C&C servers. The TOP 10 is rounded out by another newcomer, Singapore, on 2.08%.

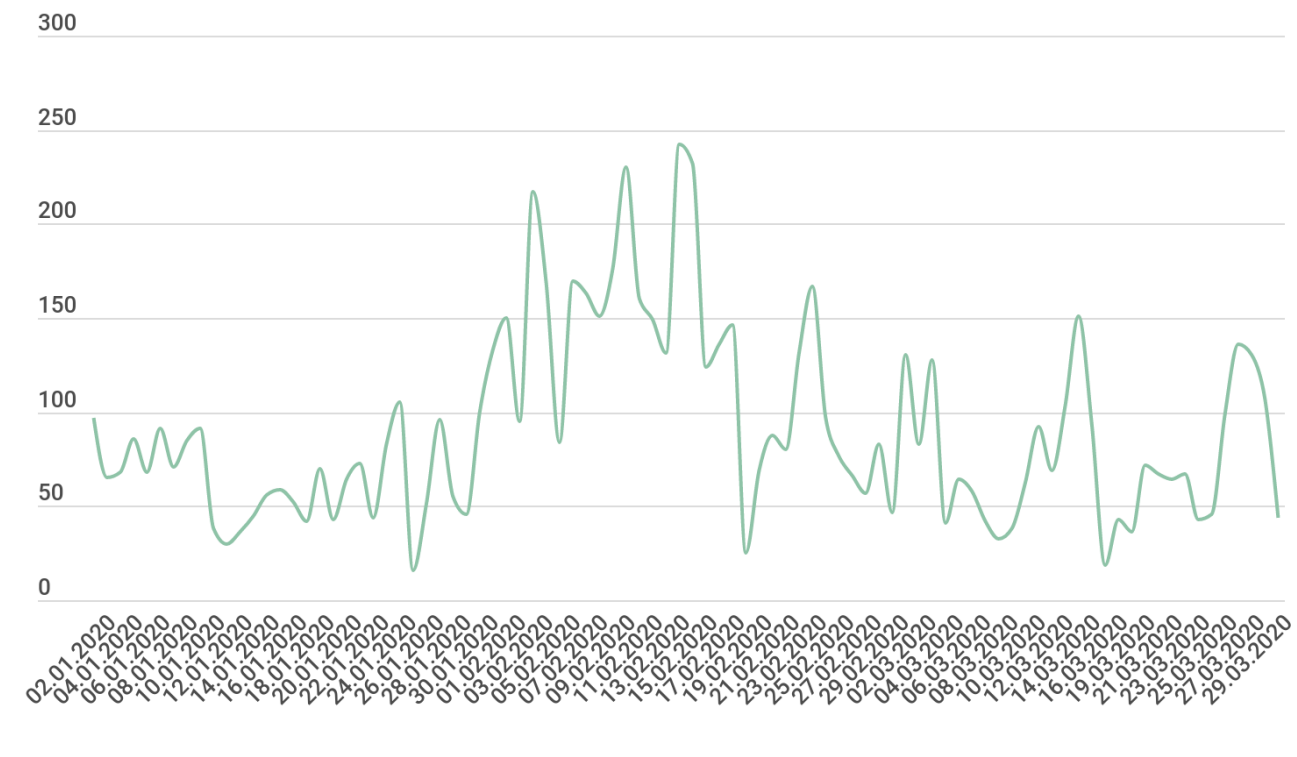


kaspersky

Distribution of botnet C&C servers by country, Q1 2020 ([download](#))

Dynamics of the number of DDoS attacks

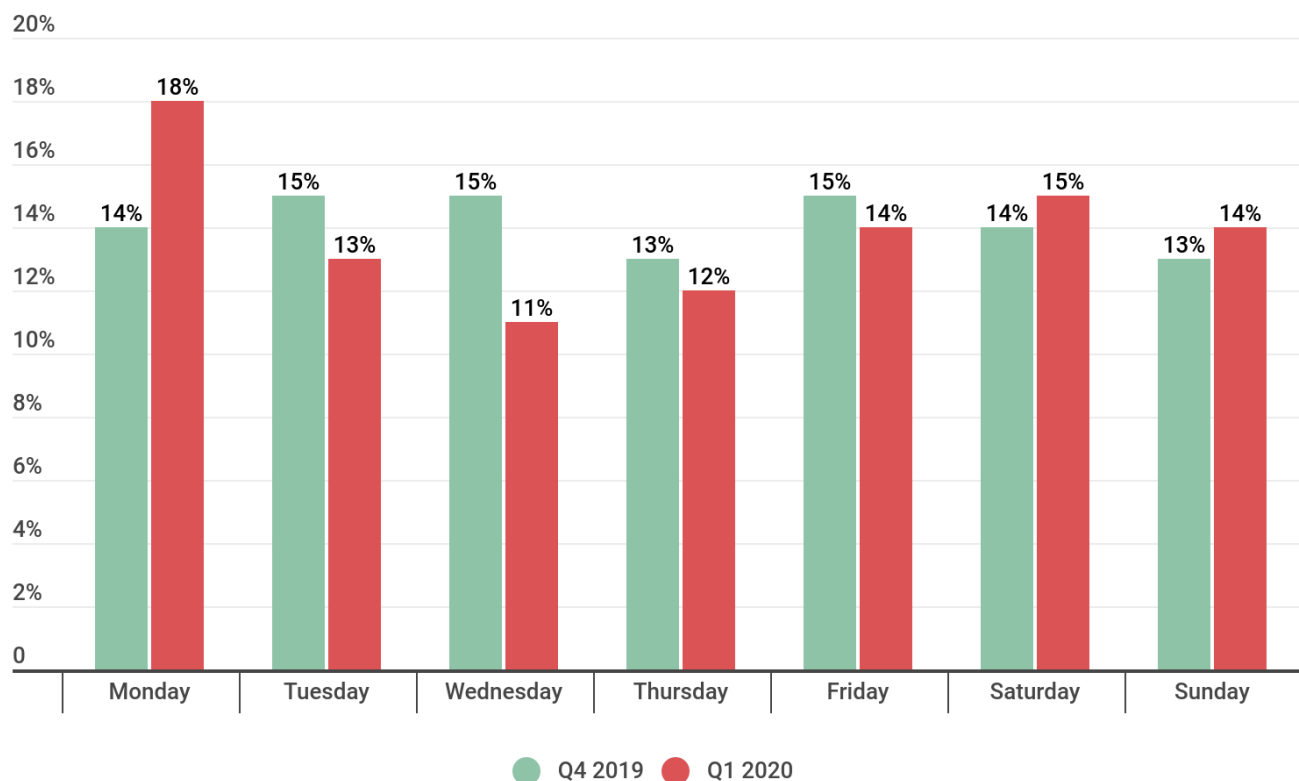
The dynamics of the number of attacks in Q1 2020 are in many ways similar to what we saw at the end of 2019. The peak indicators did not exceed 250 attacks per day (the hottest were February 14 and 15, that is, on and just after St Valentine's Day (242 and 232 attacks, respectively), as well as the 3rd and 10th of that same month). The calmest days of the quarter were January 25 and March 18, when the number of attacks fell short of 20 a day (recall that the quietest day of Q4 2019 saw only 8 registered attacks).



kaspersky

Dynamics of the number of DDoS attacks in Q1 2020 ([download](#))

In the past quarter, the number of attacks on Mondays increased significantly — by almost 4 p.p. If in the previous reporting period this day accounted for only about 14% of attacks, it now commands close to 18%. The calmest day of the quarter was Wednesday (a fraction over 11% of attacks, down 3.7 p.p. on the previous quarter), lagging only slightly behind (by 1.5 p.p.) the previous rating's anti-leader in terms of attack intensity, Thursday.

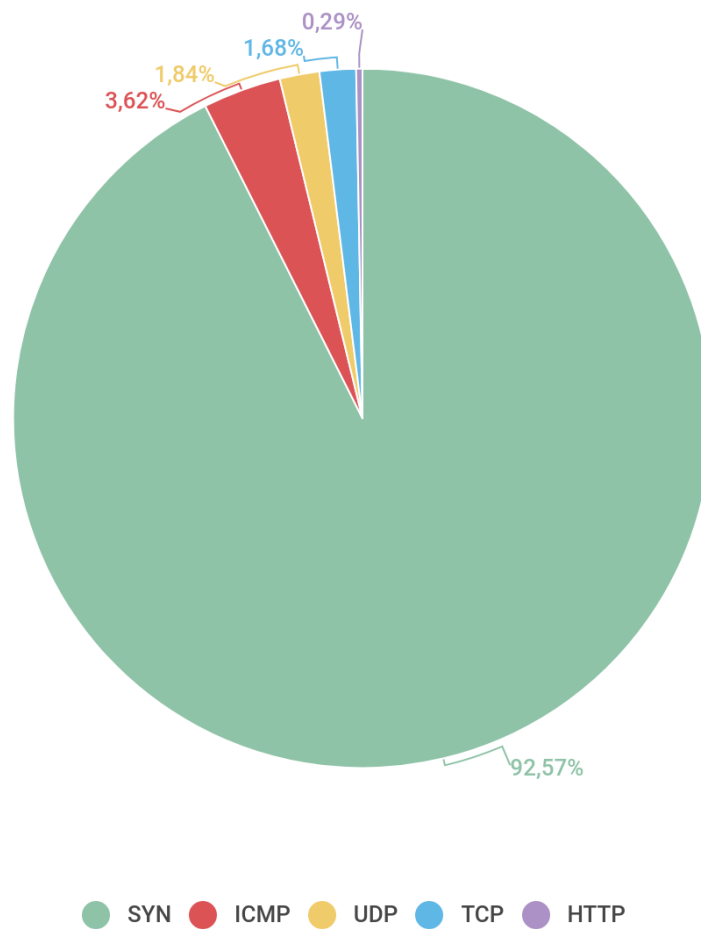


kaspersky

Distribution of DDoS attacks by day of the week, Q4 2019 and Q1 2020 ([download](#))

Types of DDoS attacks

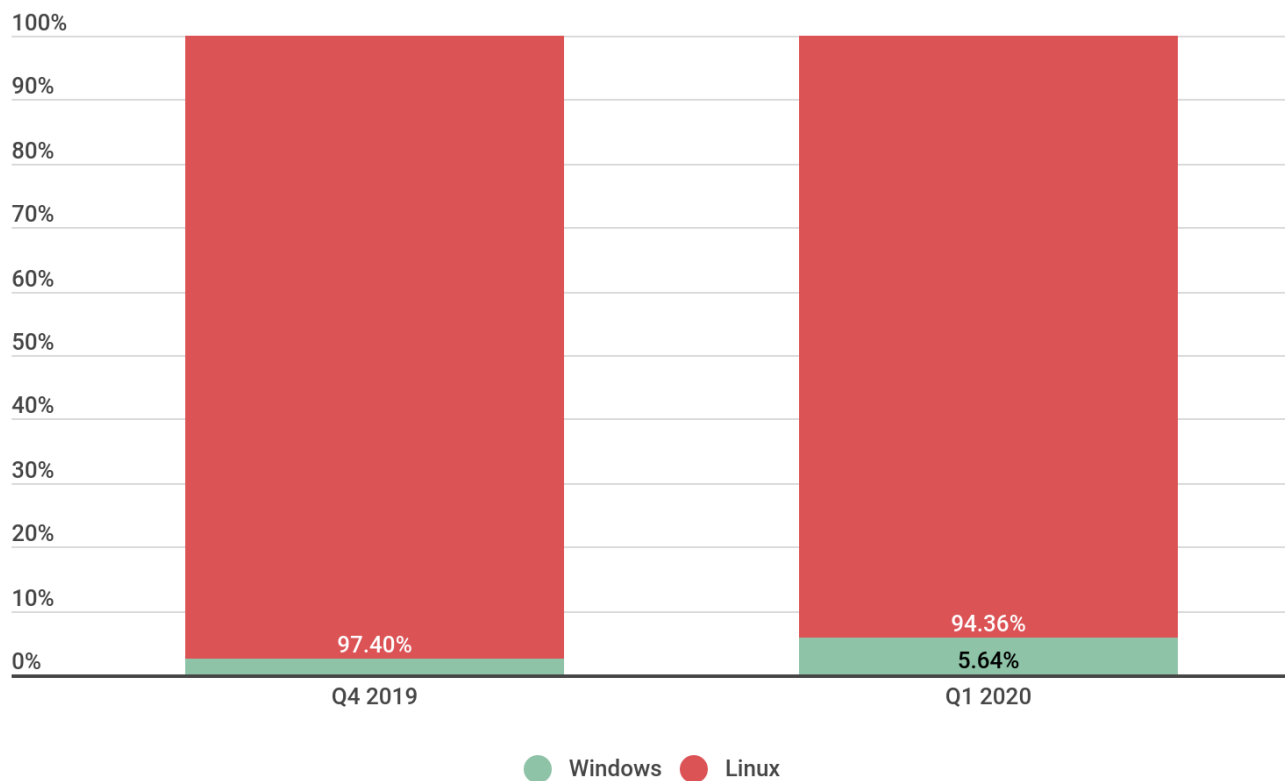
The past quarter has seen some noticeable changes in the distribution of DDoS attacks by type: ICMP flooding added 2 p.p. and confidently moved from last to second place (3.6% against 1.6% in the previous reporting period). Accordingly, HTTP flooding finished bottom with its lowest score since January 2019 (a mere 0.3%). UDP and TCP flooding once again swapped places. The only non-mover was the top-placed SYN flooding, whose share continued to grow and reached a record high of 92.6% for the observation period (beating the previous record of 84.6% set last quarter).



kaspersky

Distribution of DDoS attacks by type, Q1 2020 ([download](#))

Windows botnets are becoming more popular. If in the last reporting period they snatched just 0.35 p.p. from their Linux cousins, this time they took a 3 p.p. slice (up from 2.6% to 5.64% of attacks). That said, they are still far being a serious competitor: 9 out of 10 attacks continue to deploy Linux botnets (94.36%).



kaspersky

Ratio of Windows/Linux botnet attacks, Q4 2019 and Q1 2020 ([download](#))

Conclusion

Q1 2020 did not bring any major shocks. The TOP 10 countries by number of C&C servers welcomed two new entries (Croatia and Singapore) and saw the return of two familiar faces (Romania and Germany). Although we observed some growth in Windows botnets and ICMP floods, this did not significantly affect the overall picture. Only the distribution of attacks by day of the week changed substantially, but even that points only to a redistribution of efforts, not a quantitative shift. The rise in the number of DDoS attacks on St Valentine's Day followed by a lull was also a predictable seasonal phenomenon.

BOTNETS

DDOS-ATTACKS

INTERNET OF THINGS

Authors

Expert

OLEG KUPREEV

Expert

EKATERINA BADOVSKAYA

Expert

ALEXANDER GUTNIKOV