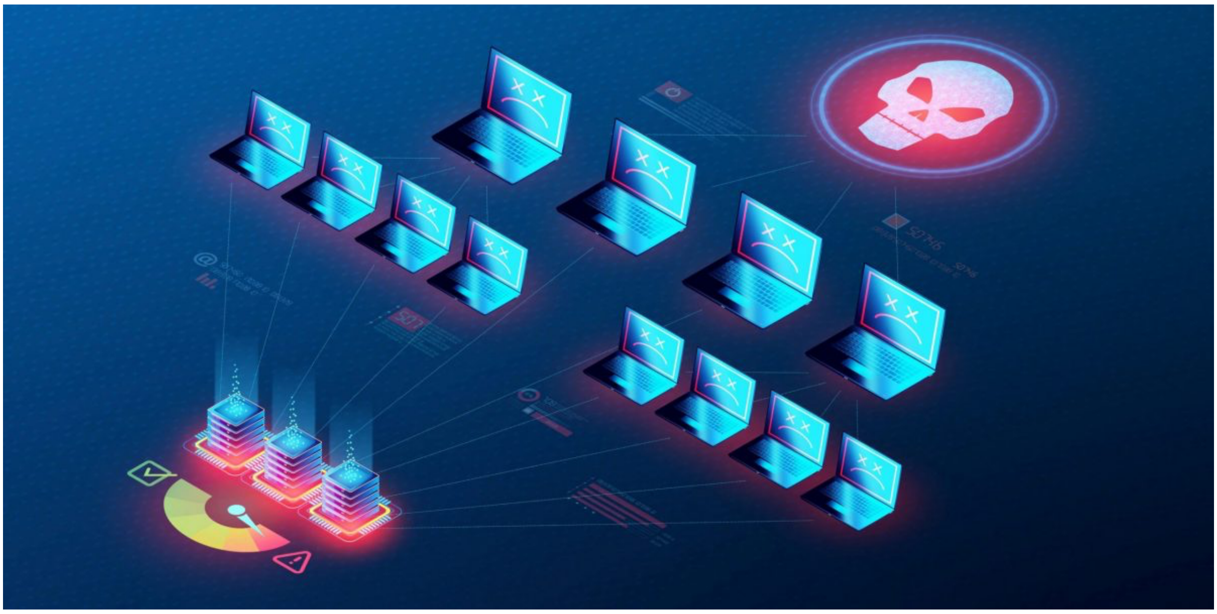
DDoS attacks in Q3 2022

DDOS REPORTS

07 NOV 2022



News overview

In Q3 2022, DDoS attacks were, more often than not, it seemed, politically motivated. As before, most news was focused on the conflict between Russia and Ukraine, but other high-profile events also affected the DDoS landscape this quarter.

The pro-Russian group Killnet, active since January 2022, took the responsibility for several more cyberattacks. According to the hacktivists themselves, more than 200 websites in Estonia fell victim to their attacks, including the ESTO AS payment system. In nearby Lithuania, the websites and e-services of the energy company Ignitis Group were hit. Both attacks were described by the affected organizations as the largest they've faced in the last 10–15 years.

Killnet also claimed responsibility for an attack on the website and services of the US Electronic Federal Tax Payment System. The attackers stated on Telegram that they were "testing a new DDoS method." During the attack, they said, the site administration tried to change the DDoS protection vendor, but then had a rethink. In addition, Killnet disrupted the US Congress website for a couple of hours.

On the other side of the Pacific, in Japan, 20 websites of four different government departments were hit by DDoS attacks. Killnet hacktivists claimed involvement in this incident, too. The defending side managed to eliminate the main damage within 24 hours, although the e-Gov administrative portal continued to experience access problems the day after.

The lesser known pro-Russian group Noname057(16) took the credit for the attacks on the website of Finland's parliament and the publication archive of its government, which they managed to take offline temporarily. If the group's Telegram channel is to be believed, the reason for the attacks was because "[Finnish] officials are so eager to join NATO."

In turn, Russian resources suffered from DDoS attacks by pro-Ukrainian hacktivists. Victims included the Unistream, Korona Pay, and Mir payment systems, as well as the Russian National Payment Card System, which ensures the operation of Mir and the Faster Payments System. What's more, activists brought down the website, call center, and SMS provider of Gazprombank; Otkritie Bank noted disruptions to its internet banking service and mobile app, and SberBank reported 450 repelled DDoS attacks in the first two months of Q3. According to SberBank, this is the same number as in the previous five years put together.

Electronic document management systems, in particular SKB Kontur and Taxcom, were also in the firing line. Their websites were either down or slow, which caused supply troubles for dairy producers. The websites of the political parties United Russia, Young Guard of United Russia, and A Just Russia — For Truth.

Media outlets did not go unaddressed either: RIA Novosti and Sputnik suffered attacks that lastedalmost 24 hours, while the website of Argumenti i Fakti was unavailable for some time. Meanwhile, StormWall reported that 70 regional newspapers in 14 Russian cities, among them Bryansk, Kaluga, Chelyabinsk, Pskov, Omsk, Tyumen, and Sochi, were hit by garbage traffic.

A wave of DDoS attacks swept across many tech and entertainment companies as well. Hacktivists attacked around 20 Russian video-conferencing platforms. Among the services affected were TrueConf, Videomost, Webinar.ru, and iMind.
Also targeted were the websites of Kinomax, Mori Cinema, Luxor, Almaz Cinema, and other movie theaters. Hacktivists also tried to disable the websites of the car information portal Drom, the drone store MyDrone, and the security vendor Avangard.

Already in Q1, various sites and apps were available to allow technically inexperienced users who sympathize with Ukraine to join DDoS attacks against Russian resources. The Russian-speaking APT group Turla exploited the hype. In July, Google researchers reported a piece of Android malware being distributed by cybercriminals under the guise of a DDoS tool for attacking Russian websites. According to experts, this is Turla's first ever malware for Android.

Besides the Russia–Ukraine conflict, there were reports of politically motivated DDoS attacks in other hot spots on the planet. US Congress Speaker Nancy Pelosi's visit to Taiwan provoked not only a public outcry in mainland China, but also a string of cyberattacks both before her arrival on the island and in the hours immediately after. In particular, the websites of Taiwan's president and its Ministry of National Defense experienced downtime. Also affected were the online resources of the Ministry of Foreign Affairs and Taoyuan International Airport.

Israel, too, became a DDoS target when cybercriminals attacked the websites of the country's Ministry of Health and Tel Aviv-Yafo Municipality. As a result, access to these resources from abroad was limited. Responsibility for the cyberattacks was claimed by Al-Tahira (aka ALtahrea), a group opposed to NATO and its allies.

The post-Soviet space was also a hotbed of activity. Amid the escalating conflict between Armenia and Azerbaijan, a DDoS attack battered the official site of the Collective Security Treaty Organization (CSTO), a Russia-led military alliance in Eurasia. The CSTO reported that attackers, under the guise of a DDoS, had attempted to change some information on its website. And in the last third of September, the Kazakhstani segment of the internet faced a DDoS onslaught from abroad. At around the same time, local media (Top Press, New Times, Skif News) were also subjected to DDoS attacks.

Some events in Q3 could not be described as unambiguously political. For example, the company Russian Environmental Operator reported DDoS attacks on the new Secondary Material Resources Exchange immediately after the announcement of the platform's launch. Although this may have been part of a hacktivist campaign, new online resources regularly face DDoS attacks before going live even during quiet times. The largest Russian-language torrent tracker RuTracker and the entertainment portal Live62 also admitted to being attacked in Q3. Both sites have been beset by copyright infringement claims, and RuTracker has been blocked in Russia as a pirate resource.

In addition, a number of firms specializing in DDoS protection reported major attacks in Q3.

Akamai announced two major attacks on the same client from Eastern Europe. In both cases, the number of packets per second sent by the attackers was extraordinary. The first attack, on July 21, peaked at 659.6 million packets per second, a new European record at the time, says Akamai. This was not an isolated case: in July, this same client was attacked more than 70 times. The record held until September 12, when another attack posted 704.8 million packets per second.

In continuation of a Q2 trend, Google says it blocked an HTTPS-based DDoS attack that peaked at 46 million requests per second, 77 percent more than the record-breaking HTTPS attack mentioned in our previous report. According to experts, the attack involved more than 5,000 IP addresses from 132 countries, with around 30 percent of the traffic coming from Brazil, India, Russia, and Indonesia. The geographical distribution and botnet characteristics suggest the use of the Mēris family.

Lumen reported stopping an attack with a capacity of over 1 terabyte per second on the servers of its client. At the time of the attack, the target servers were hosting a gaming service. In the week leading up to the incident, the attackers tested various DDoS methods and studied the victim's protection capabilities by issuing commands to bots from three different C2 servers.

Gaming services are regularly targeted by DDoS. In Q3, the servers of Gaijin Entertainment, which developed *War Thunder*, *Enlisted*, and *Crossout*, were hit by an extended series of attacks. They began on September 24, and users were still complaining of disruptions at the time of writing. To reduce the negative effect of the DDoS attack, Gaijin promised to extend its promotions and premium subscriptions, as well as award bonuses to players for a whole week.

The North American data centers of *Final Fantasy 14* were attacked in early August. Players experienced connection, login, and data-sharing issues. Blizzard's multiplayer games — *Call of Duty*, *World of Warcraft*, *Overwatch*, *Hearthstone*, and *Diablo: Immortal* — were also DDoSed yet again.

An ESL eSports match between the teams NaVi and Heroic was held up for over an hour due to a DDoS attack on individual players. The match continued only after the organizer had dealt with the threat.

In turn, the developers of the game *Tanki Online* announced they had finally neutralized a string of DDoS attacks that had plagued players since the summer. Having beefed up protection and stabilized the servers, the organizers thanked the players for their patience with a prize giveaway.

That was not the only good news regarding DDoS attacks on gaming services this quarter: in Sweden, police detained a suspect in a DDoS attack on Esportal, a *CS:GO* tournament platform. If convicted, they face from six months to six years in prison.

Anti-DDoS measures are also being implemented at the national level. For instance, Israel announced the launch of the Cyber-Dome project, designed to secure national digital resources. According to the Israel National Cyber Directorate, having a single protective complex will "elevate national cybersecurity by implementing new mechanisms in the national cyber perimeter and reducing the harm from cyberattacks at scale."

In Bangladesh, the governmental Computer Incident Response Team required all key organizations, including those responsible for the country's IT infrastructure, to develop and introduce anti-DDoS measures. This came after a reported spike in attacks.

At the same time, the global legal consensus that any DDoS attack constitutes a cybercrime came under threat in Q3, and from an unexpected source. The Hungarian Cable Communications Association (MKSZ) requested that the law be changed to officially allow MKSZ members and legal enterprises from the telecom industry to carry out DDoS attacks as a means of combating IPTV piracy. Traditional measures, such as blocking IP addresses and domain names, MKSZ described as slow and ineffective, while legally sanctioned cyberattacks could genuinely force users to abandon pirate services.

It was not only Hungarian telecom companies that had the idea of taking the fight to cybercriminals. After the ransomware group LockBit hacked Entrust, a specialist cybersecurity firm, and began publishing confidential data, unknown actors attacked the site where the information was being leaked. The packets they sent contained an unambiguously worded message: DELETE_ENTRUSTCOM_[BAD_WORD].

Quarter trends

The main surprise of Q3 2022 was the lack of surprises, which were continuously present since late 2021. But that doesn't mean it was a dull quarter. Let's take a look at the statistics.

Comparative number of DDoS attacks, Q3 2021, Q2 and Q3 2022. Q3 2021 data is taken as 100% (download)

The first thing worth noting is the significant rise in the number of DDoS attacks of all types relative to the previous reporting period. At the same time the quarter picture is fairly standard: a relatively calm summer followed by a sharp surge in DDoS activity. In September, the Kaspersky DDoS Protection team repelled 51 percent of all attacks in the quarter, which amounts to roughly the same number as in the previous two months. This is a normal situation that we observe and report on every year. Usually the autumn growth is more of a recovery after the summer slump, but the fact remains that the number of DDoS attacks always increases sharply in September. This is due to a general rise in activity after the lazy summer months: people return from vacation, students go back to school, and everything picks up, including the DDoS market.

Share of smart attacks, Q3 2021 and Q2/Q3 2022 (download)

What is unusual, however, is the continued growth in the share of smart attacks, which, with 53 percent, already account for the majority, setting a new record in the history of our observations. Moreover, DDoS attacks on HTTP(S) this quarter exceeded those on TCP for the first time, despite the latter being easier to organize and still the most common type of DDoS.

Ratio of HTTP(S) and TCP attacks, Q2 2021–Q3 2022 The number of TCP-based attacks for the corresponding period is taken as 100% (download)

What's most interesting is that, in absolute terms, the number of attacks on HTTP(S) has remained quite stable over the past year. The share of attacks on TCP is on a downward curve, which reflects well the general trend: the share of dumb DDoS attacks is falling, while that of smart attacks is growing. This was bound to happen sooner or later, as tools on both the attacking and defending sides evolve and become more readily available. Organizing L7 attacks is getting easier, while L4 attacks are losing their effectiveness. As a result, they are being used less and less by professionals in their pure form (although L4 vectors are still found in mixed attacks), and more and more by amateurs. The above figures illustrate this well.

Note this Q1 2022 stat: There were half as many DDoS attacks on HTTP(S) as on TCP. February and March saw a significant increase in non-professional attacks due to the geopolitical situation, as outlined in our report. Hacktivists are passionate but fickle. Having quickly tired of DDoS, they switched to other attacks, and the share of DDoS started to fall. By Q3, it was tending to zero. Meanwhile, the number of high-quality professional attacks, after increasing in Q1, remains at a high level. The targets have not changed either: mainly the financial and government sectors. Both of these facts reinforce our notion that, from the spring until at least the end of September, professionals were working to order against these sectors, which is reflected in our statistics.

In terms of DDoS attack duration, there were no new records: if Q2 was marked by the longest attack ever observed, Q3 was calmer: on average, attacks lasted about eight hours, with the longest being just under four days. Compared to the previous quarter, this seems rather modest, but the numbers are still huge: in Q3 of last year, the duration of DDoS attacks was measured in minutes, not hours. In this regard, the situation remains challenging.

DDoS attack duration, Q3 2021 and Q2/Q3 2022. Q3 2021 data is taken as 100% (download)

DDoS attack statistics

Methodology

Kaspersky has a long history of combating cyberthreats, including DDoS attacks of varying 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 Q3 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 Q3 2022:

- Kaspersky's DDoS Intelligence system detected 57,116 DDoS attacks.
- A total of 39.61 percent of targets, affected by 39.60 percent of attacks, were located in the US.
- The busiest day of the week (15.36 percent of attacks) was Friday and the calmest (12.99 percent) was Thursday.
- July saw the sharpest contrast: The 1st and 5th saw 1494 and 1492 attacks, respectively, and the 24th just 135.
- Attacks lasting less than four hours accounted for 60.65 percent of the total duration of attacks and for 94.29 percent of the total number of attacks.
- UDP flood accounted for 51.84 percent of the total number of attacks, and SYN flood for 26.96 percent.
- The country with the largest share of bots trying to hack into Kaspersky SSH honeypots was the US (17.60%).

DDoS attack geography

In Q3 2022, the top four countries in terms of resources attacked remained unchanged from the previous reporting period. The US (39.60%) remained in first place, despite losing 6.35 percentage points. Mainland China's share (13.98%) increased by almost the same amount, up 6.31 percentage points, securing second place. Germany (5.07%) remains in third and France (4.81%) in fourth place.

Hong Kong (4.62%) rounded out the TOP 10 countries and territories with the highest number of DDoS attacks last quarter. Having seen its share more than double this quarter, it now ranks fifth. Brazil (4.19%) moved up into sixth position, while Canada (4.10%) and the UK (3.02%), which ranked fifth and sixth last quarter, dropped to seventh and eighth, respectively. Propping up the TOP 10 are Singapore (2.13%) and the Netherlands (2.06%).

Distribution of DDoS attacks by country and territory, Q2 and Q3 2022 (download)

The distribution of unique DDoS attack targets by country and territory is almost a carbon copy of the attack rating. In first place is the US (39.61%), followed by mainland China (12.41%), whose share grew most noticeably over the quarter, up 4.5 percentage points. Third place still belongs to Germany (5.28%), and fourth to France (4.79%).

As in the distribution of attacks, Brazil (4.37%) and Hong Kong (4.36%) ranked fifth and sixth by number of unique targets, but in reverse order. The former was home to slightly more DDoS targets, while the latter showed larger growth against the previous reporting period, climbing 2.36 percentage points. Canada (3.21%), the UK (2.96%) and Singapore (2.11%) occupied lines seven to nine in the table, while tenth place went to Poland (2.00%), squeezing the Netherlands (1.86%) out of the TOP 10.

Distribution of unique targets by country and territory, Q2 2022 and Q3 2022 (download)

Dynamics of the number of DDoS attacks

The number of DDoS attacks in Q3 2022 fell again. Having decreased by 13.72 percent in the previous reporting period relative to the one before, this quarter it dropped by a further 27.29 percent, to 57,116. August proved to be the busiest month, with Kaspersky's DDoS Intelligence system detecting an average of 824 attacks per day. July, on the other hand, was calm: 45.84 percent of all attacks during this month occurred in the first seven days, maintaining the dynamics of June, which posted an average of 1301 per day; starting from week two, however, the average number of daily attacks fell to 448. Thus, the July average was just 641 DDoS attacks per day, slightly ahead of the even quieter September, which averaged 628.5. At the same time, September's attacks were distributed more evenly throughout the month.

The quarter's peak and trough both came in July: the most aggressive day was the 1st (1494 attacks); the calmest was the 24th (135). In August, over a thousand attacks were recorded on the 8th and 12th alone (1087 and 1079, respectively), and the quietest day was the 30th (373). September delivered no noteworthy highs or lows.

Dynamics of the number of DDoS attacks, Q3 2022 (download)

Sunday (13.96%) in Q3 fell by 1.85 percentage points compared to the previous reporting period, and lost its position as the leading day in terms of traffic. Saturday's share also declined, but remained above 15 percent. First place by number of DDoS attacks went to Friday, which showed a noticeable increase — from 13.33 to 15.36 percent. Thursday was the only day whose share dropped below 13 percent, down to 12.99 percent.

Distribution of DDoS attacks by day of the week, Q3 2022 (download)

Thursday was also the only weekday that saw its share decrease.

Duration and types of DDoS attacks

In Q3 2022, sustained attacks of 20 hours or more accounted for 19.05 percent of the total duration of attacks. This figure almost tripled after falling in the previous reporting period, almost reaching the level as that at the beginning of the year. Accordingly, the proportion of long-term attacks increased quantitatively: from 0.29 to 0.94 percent.

Short attacks lasting up to four hours showed a slight decrease to 94.29 percent. At the same time, their share of the total duration of DDoS attacks fell significantly, from 74.12 to 60.65 percent. Attacks lasting from five to nine hours remained in second place (3.16% of attacks); attacks lasting from 10 to 19 hours were in third (1.60%).

The longest attack of Q3 lasted 451 hours (18 days 19 hours). That was way ahead of the second-place 241 hours (10 days 1 hour). The average duration of attacks rose slightly to around 2 hours 2 minutes, which is not surprising given the increase in the share of sustained attacks and the decrease in the share of short ones.

Distribution of DDoS attacks by duration, Q2 and Q3 2022 (download)

In Q3 2022, the ranking of DDoS attack types was unchanged from the previous reporting period. The share of UDP flood fell from 62.53 to 51.84 percent, but remained the most common type of DDoS. The second most common, SYN flood, on the contrary, increased its share to 26.96 percent. TCP flood (15.73%) reversed its decline, adding more than 4 percentage points to hold on to third place. GRE flood and HTTP flood made up 3.70 and 1.77 percent, respectively, of the total number of attacks.

Distribution of DDoS attacks by type, Q3 2022 (download)

Geographic distribution of botnets

Botnet C2 servers are still mainly located in the US (43.10.%), but its share fell by 3 percentage points. The Netherlands (9.34%), which ranked second last quarter, slipped more than 5 percentage points and again changed places with Germany (10.19%). Russia (5.94%) stayed in fourth place.

Asian countries come next: fifth place goes to Singapore (4.46%) and sixth to Vietnam (2.97%), whose share in Q3 continued to grow, although not as rapidly as in Q2. They are followed by a new entry in the ranking, Bulgaria (2.55%), whose share increased more than sixfold.

France dropped from fifth place to eighth (2.34%), and the UK (1.91%) to ninth. Canada and Croatia, which rounded out last quarter’s TOP 10, gave way to Hong Kong (1.49%) by number of C2 servers.

Distribution of botnet C2 servers by country and territory, Q3 2022 (download)

Attacks on IoT honeypots

In Q3, mainland China surrendered its lead in terms of number of bots attacking Kaspersky SSH honeypots: its share dropped to 10.80 percent. First place was claimed instead by US-based bots (17.60%). Third, fourth, and fifth positions, with hardly any distance between, belong to India (5.39%), South Korea (5.20%), and Brazil (5.01%). Germany (4.13%) dropped from third place last quarter to seventh, but bots based there were among the most active in Q3, responsible for 11.22 percent of attacks. This figure is bettered only by the US bots (27.85%). What’s more, over five percent of attacks came from bots in Singapore (5.95%) and India (5.17%), which took third and fourth place, respectively.

TOP 10 countries and territories by number of devices from which Kaspersky SSH traps were attacked, Q3 2022 (download)

As for Kaspersky Telnet honeypots, here mainland China retained its lead among countries and territories by number of both attacks and attacking devices. The first figure, however, declined from 58.89 to 38.18 percent, while the second climbed slightly from 39.41 to 41.91 percent. Second place by number of attacks went to the US (11.30%), with Russia third (9.56%). In terms of their share of bots, these two countries rank slightly lower: in sixth (4.32%) and fourth (4.61%) place, respectively. The TOP 3 countries by number of bots featured South Korea (8.44%) and India (6.71%). Taiwan ranked fifth with 4.39 percent.

TOP 10 countries and territories by number of devices from which Kaspersky Telnet traps were attacked, Q3 2022 (download)

Conclusion

The situation in Q3 2022 points to a stabilization of the DDoS market after a tumultuous first half of the year, although it remains difficult. Yet the picture changes every quarter and forecasts remain tentative at best: pretty much anything can happen. That said, we don’t expect any significant surges or drops in Q4. If our conclusions are correct, and the market is indeed back on a predictable track, we expect similar indicators in Q4 as in Q3, adjusted for the slight growth we usually see toward the end of the year. In any case, we can assume such a development in terms of both number and quality of attacks. As for duration, here we can only guess: the DDoS market is still very far from the norm, and the length of attacks tends to jump up and down. We hope that Q4 shows relative stability in this regard, too, and does not try to break any records.