SECURELIST by Kaspersky

DDoS attacks in Q2 2022

News overview

Politically-motivated cyberattacks dominated the DDoS landscape in the second quarter of 2022 just as they did in the previous reporting period. ALtahrea Team, a group targeting NATO and its partners, attacked public transportation websites in Israel and the United Kingdom. Israel saw a cyberattack on the Airports Authority, and UK, an attack on the Port of London Authority. Also attributed to the group are cyberattacks on websites affiliated with the Turkish ministry of defense.

Attacks linked in some way or another to the Russia-Ukraine conflict continued too. The pro-Russian hacktivists Killnet, which first surfaced in January 2022, claimed responsibility for DDoS attacks on the websites of various European organizations from April through June. Starting on April 18, Czech government and public transportation websites, including those of the rail authority and airports, came under attack. Then on April 29, the hackers targeted Romanian government websites including those of the Border Police, the National Railway Transport Company and Optbank, and on May 8, German websites, including the Bundestag and the Federal Police. Italy was another DDoS target: the websites of the senate, the National Health Institute and the Automobile Club d'Italia took a hit on May 11. The attackers used the slow HTTP technique, transmitting the HTTP request body at a very low rate and sending incomplete requests to make the target servers allocate resources for listening. Later cyberattacks attributed to Killnet affected the Italian foreign ministry and national magistrate association websites. In late June, the hacktivists attacked Lithuania's Secure National Data Transfer Network as well as

other government agencies in that country. At various points throughout the quarter, the group took responsibility for DDoS attacks on various European organizations, which did not publicly confirm the incidents.

In several cases, no entity claimed responsibility for what was presumed to be politically-motivated attacks. For example, websites belonging to the Vltava Labe Média publishing house were down on April 6–7. The publisher said it had been subjected to DDoS attacks multiple times since the start of the Ukraine conflict. The websites of Finland's defense and foreign affairs ministries were unaccessible on April 8, the day when Volodymyr Zelenskyy was addressing the country's parliament. Iceland was the target of several cyberattacks in mid-April, with the websites of various organizations affected, including media outlets. The police suspect political motivation as the country announced the intention in March to boost its defense budget. Some of the targeted resources resorted to geoblocking to stay online.

Another anonymous attack that could be categorized as driven by political motives is the April 22 DDoS attack on Ukraine's postal service, which followed the release of postage stamps featuring the image of the Russian cruiser Moskva. Estonian government websites, including the Information System Authority (RIA), remained under attack from April 21 through at least April 25. The Estonian government came under attack again on May 9 as the website of the country's foreign ministry was brought down.

Some of Ukrainian and pro-Ukrainian websites were attacked from compromised WordPress sites. Hackers were embedding a script within the main files of the websites, which sent requests to various targets on behalf of visitors. In technical terms, this bore a similarity to the hacktivist attacks on Russian websites that we covered in the first quarter, the difference being that in the earlier case, the hacktivists were making DIY stresser sites, allowing sympathetic visitors to aid in their DDoS efforts. Interestingly enough, one of the hacked WordPress sites was a hacktivist website used to attack Russian media outlets in the previous quarter.

Russian websites remained a target for DDoS attacks in Q2. The attacks were coordinated via pro-Ukrainian Telegram channels as before. A hacktivist attack on the information systems that supported the St. Petersburg International Economic Forum (SPIEF) resulted, among other things, in the Russian president's speech at the event being delayed by an hour. The SPIEF press pass issuance system and press room experienced issues too.

A further DDoS target was the Gosuslugi e-government website and mobile application. Russia's ministry of digital development reported a tenfold load increase on these resources. Other federal agencies subjected to cyberattacks were the consumer health watchdog Rospotrebnadzor and the agricultural safety watchdog Rosselkhoznadzor. The latter's website said the cybercriminals were primarily targeting Mercury, an electronic veterinary certification system.

Other electronic document management systems were targeted too. Alcohol producers and distributors faced difficulties delivering their goods to stores due to a cyberattack on the Unified State Automated Information System (EGAIS). Due to

outages that affected the fiscal data operator's website, OFD.ru, receipt delivery to internal revenue offices was greatly delayed. The Chestny ZNAK national track & trace digital system was also inundated with junk traffic.

Websites of the Perm Krai provincial administration and legislature were among the government resources that suffered from cyberattacks. The hacktivists haven't spared the media either: novgorod.ru, Zebra TV, Amurskaya Pravda, sibkray.ru, the Lotos state broadcaster and other provincial news outlets reported service disruptions.

Private service providers were also caught in a surge of cyberattacks. According to CNews, 1C-EDO, 1C-OFD, 1C:Reporting and other services of Russian enterprise software developer 1C were unavailable for several days. The privately-owned RosDorBank recorded an impressive volume of malicious traffic: up to three million requests per second. A number of Russian airlines — Rossiya, Aurora, ALROSA, and others — said around the same time that their websites had been targeted by DDoS attacks. "Moskovskiye apteki", a pharmaceutical journal, reported that aptekamos.ru and other websites of well-known pharmaceutical publications and pharmacy aggregators and chains had been attacked daily from March through June.

NashStore, Russia's mobile app marketplace modeled after App Store and Google Play, experienced outages on its official launch day. Widespread DDoS attacks targeted Russian colleges as enrollment boards began to examine applicants. Outages affected visitors to some websites of RUDN University and Moscow Polytechnical University, Astrakhan State University, Siberian Federal University, colleges in Yaroslavl, Perm and Irkutsk, and schools in Tatarstan, the Komi Republic, Altai Krai, Amur Oblast and other provinces. Students are often known to be behind DDoS attacks on schools, especially on key academic dates, but in this case, the cyberattacks were orchestrated via pro-Ukrainian Telegram channels too.

Educational establishments in the United States suffered from DDoS attacks as well: schools of Topeka USD 501, Kansas, were disconnected from the internet for five minutes as a result of a cyberattack. The incident prompted the school district administration to contract a specialized infosec provider for DDoS protection.

As usual, the gaming industry was targeted too. Fans of World of Warcraft, Overwatch, Call of Duty and Diablo III had issues accessing the games for slightly more than an hour on May 11 as Battle.net experienced a DDoS attack on its servers. STEPN, a game in which players can earn crypto tokens for real-life running and trade in virtual sports shoes, reported a series of incidents in June. The attacks followed an update that targeted cheaters. The admins asked the users to take a break from the game to avoid errors in recording their workouts.

DDoS attacks on websites associated with cryptocurrency are anything but rare. They are often timed to coincide with landmark events, such as new cryptocurrency launches and rate fluctuations. In Q2 2022, the website of the Tether stablecoin was targeted by a DDoS attack after the rate dropped despite USD pegging.

Ransom DDoS attacks, which often made the news in 2020 and 2021, had all but died down: the only one that received broad coverage was an attack by a group that claimed to be the operator behind the infamous REvil ransomware. Our fellows at Cloudflare acknowledged the trend in their Q1 2022 report.

Cloudflare also reported two unprecedentedly powerful HTTPS DDoS attacks. These are more costly both to the attacker and the victim compared to DDoS attacks that use the unsecured HTTP protocol. In the first case, the attack rate reached 15 million requests per second, with the target bombarded with junk traffic for less than 15 seconds. The victim was a company operating a crypto launchpad. The record was beaten two weeks later by an attack with the magnitude of 26 million requests per second.

Both attacks were launched by relatively small botnets consisting of five to six thousand devices each. Unlike larger, but less powerful zombie networks composed of IoT devices, these utilized web servers and virtual machines. The operator behind the second HTTPS attack, the most powerful one to date, has been nicknamed Mantis after the tiny yet mighty predatory insect.

Botnets built from routers, cameras, and other consumer devices did not go away, either. The 360 Netlab company published a report on a new zombie net named Fodcha, which expanded through brute-force attacks and by exploiting known vulnerabilities in IoT devices. As of April 10, 2022, the number of Fodcha bots in China alone exceeded 60 000, with more than 10 000 active daily. Fodcha C2 servers were originally hosted on a single cloud provider's network, but after those were blocked, the operators had to rebuild their infrastructure. At the time the study was published, command and control functions were spread across several providers' clouds, with commands reaching bots from a dozen IP addresses in different countries.

Enemybot is another new DDoS botnet, which belongs to the Keksec extortion group, borrows code from the Mirai and Gafgyt bots, and drops a file with the cybercriminals' signature on devices it infects. The bot specializes in attacking routers and web servers that contain known vulnerabilities, including those discovered in 2022.

As for previously-known botnets, Q2 2022 saw a series of publications on their recent activity. Fortinet reported in early April on two vulnerabilities, which were weaponized by the Mirai variant known as Beastmode. A significant portion of these were vulnerabilities found in TOTOLINK routers in 2022. In May, Microsoft published a report on a surge in activity associated with the XorDdos bot that targets Linux devices.

Another noteworthy publication appeared on Stackoverflow: On May 16, the website posted a breakdown of cyberattacks it suffered, describing some interesting techniques and explaining how Stackoverflow had defended itself. For example, in one of the cases, the attackers used highly expensive SQL queries triggered from a large number of IP addresses. This meant that IP blocking was not an effective

protection method, and the criminals managed to load some of the backend servers to full capacity.

Positive Technologies and Qrator Labs experts said the second quarter saw a new trend among DDoS attackers: they began looking for ways to bypass geoblocking after companies started to rely heavily on the technique. In particular, they use VPN, proxy servers, and infected devices located in the same region as the target to render blocking pointless.

Amid the battle between the attackers and their targets, Roskomnadzor, Russia's communications watchdog, said it would adopt the Deep Packet Inspection (DPI) technique to fight DDoS. Critics say that although technically feasible, DPI is limited in what it can do and is no cure-all. Besides, the system would need to be updated and trained to make it fit the purpose.

Meanwhile, other countries keep on combating operators renting out DDoS capacities: the FBI, supported by Dutch and Belgian authorities, seized two domains used for selling the services.

Quarter trends

The second quarter of 2022 saw the continuation of a trend that began in spring: an increase in superlong attacks. These last so long that websites remain under stress continuously. Compared with the previous quarter, DDoS attacks faded from public view and amateur hacktivist attacks all but ceased. That said, they had done no major damage before, so the cessation had little effect from a DDoS defense perspective. But let us look at the figures.

Comparative number of DDoS attacks, Q2 2021, Q1 and Q2 2022. Q2 2021 data is taken as 100% (download)

In this quarter, the Kaspersky DDoS Protection group repelled about 2.5 times more attacks year-on-year. The number is huge, but it pales in comparison with Q1 2022 when we detected almost twice as many. It would seem that we are seeing a drop in attacker activity, but things are, in fact, much more interesting. Though there were fewer attacks in absolute terms, the overall DDoS situation might have deteriorated.

As mentioned above, hacktivist activity, which was responsible for the previous quarter's surge, tapered off. An overwhelming majority of those attacks were neither professionally managed nor very long, so they failed to produce any particular effect on anything but pure statistics. The attacks we observed in Q2 and are still observing are of a somewhat different nature. They last for days, even weeks, with this quarter's record being 41 441 minutes or about 29 days. The most attacked resources remain stressed almost continuously.

DDoS attack duration, Q2 2021, Q1 and Q2 2022. Q2 2021 data is taken as 100% (download)

The average duration of a DDoS attack in Q2 was about 3000 minutes (roughly 50 hours or about 2 days). Compare this with the average of 30 minutes for Q2 2021: the figure has grown hundredfold. It is extremely expensive to sustain an attack for such a long time, especially an ineffectual attack that gets blocked by cybersecurity systems. Continuous bot activity increases the risk of botnet hosts wearing out or being detected, or even the C2 center itself getting traced. The fact that these attacks do happen makes one wonder what the operators' true capabilities and affiliations are.

In terms of DDoS attack quality, we are seeing a trend for greater complexity. The share of smart attacks in Q2 2022 almost reached 50%, which is close to a record. The figure was last that high when the DDoS market was at rock bottom about four years ago. The rise began with expensive, well-staged attacks. It is fairly unusual to see a figure like that in a DDoS-rich year.

Share of smart attacks, Q2 2021, Q1 and Q2 2022 (download)

More interestingly, Q2 2022 saw a large number of high-class targeted attacks, which are designed for a specific website, with its features and vulnerabilities in mind. These are very expensive, very complex attacks that require a high standard of competence and extensive knowledge from both the attackers and the defending party. Normally, these occur in single-digit numbers, so even one attack in a year is a remarkable occurrence. In the second quarter, we saw two. This is quite an alarming trend, which makes one wonder what size of resources these cybercriminals command.

Another, extremely important, trend of the second quarter is the crypto crash, which began with an instant Terra (Luna) collapse and has only intensified ever since. As we and our peers have noted in multiple posts, the DDoS market is highly sensitive to crypto market fluctuations and inevitably grows when crypto declines. We have not seen crypto collapse this rapidly for a long time, and by all indications, this will last: for example, miners have started selling off their farms to gamers. It is not unreasonable to expect the DDoS market to start growing soon. The DDoS situation in Russia is already about as tense as it gets, so we are unlikely to notice any changes in that region. On a global scale, there is a high probability that DDoS activity will intensify.

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 Q2 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 Q2 2022:

- Our DDoS Intelligence system recorded 78,558 DDoS attacks.
- 25% of the targets were located in the US, accounting for 45.95% of all attacks.
- June 20 and 21 were the wildest days, with 1815 and 1735 attacks, respectively, while April 10 and 11, and May 17 were the least turbulent ones, with 335, 294 and 267 attacks, respectively.
- Very short attacks made up 95.42% of the total number.
- 17% of the botnet C2 servers were located in the US.
- UDP flood accounted for 62.53% of attacks.
- 41% of the devices that attacked Kaspersky Telnet honeypots were located in China.

DDoS attack geography

The US remained the leader in the number of DDoS attacks on the country's resources, with their share of the total rising slightly to 45.95% from the first quarter's 44.34%. China was still the runner-up with 7.67%, but the country's share dropped by 3.93 p.p. Germany came up close with 6.47%, gaining 1.41 p.p.

Distribution of DDoS attacks by country and territory, Q1 and Q2 2022 (download)

A sharp drop in attacks on the Hong Kong special administrative region (to 1.75%) continued for a third consecutive quarter. After its share more than halved yet again, the territory found itself in tenth place, virtually matching its position in Q2 2021. France and Canada displayed minimal gains, with 4.60% and 3.57%, respectively, inheriting the UK's and Hong Kong's fourth and fifth places. Great Britain sunk to sixth place with 3.51%, followed by Brazil with 3.2% and the Netherlands with 2.91%.

Coming up close in ninth place was Singapore, the only country of the TOP 10 besides the US and Germany to see attacks grow by more than one percentage point, to 2.9% from 1.86%.

Singapore's share of unique targets (3.22%) grew even more noticeably, more than doubling from Q1 2022. As a result, the country, which was not even among the ten leaders at the beginning of the year, found itself in sixth place. Overall, the composition of the TOP 10 is traditionally similar to the rankings by the number of attacks. The three leaders remained unchanged: the US (43.25%), China (7.91%) and Germany (6.64%). France rose to fourth place with 4.42%.

Distribution of unique targets by country and territory, Q1 and Q2 2022 (download)

Hong Kong (2.01%) dropped from fifth place to tenth as the UK (3.77%) slid by one position to take its place. Other members of the TOP 10 included Brazil (3.18%) in seventh place, Canada (2.97%) and the Netherlands (2.73%).

Dynamics of the number of DDoS attacks

In Q2 2022, DDoS attacks dropped by 13.72% (to 78 558) as compared to the previous reporting period. Activity increased steadily throughout the quarter: from 731 attacks per day on the average in April to 845 in May, to 1195 in June. June 20 and 21 proved to be the busiest, with 1815 and 1735 attacks, respectively, whereas April 10 and 11 were the calmest, with the Kaspersky DDoS Intelligence system recording 335 and 294 attacks, respectively, and May 17, when we saw just 267 attacks.

Dynamics of the number of DDoS attacks, Q2 2022 (download)

The distribution of DDoS attacks by day of the week was slightly more even than in Q1 2022. Friday (13.33%) grew by 0.56 p.p., passing its title of the calmest day to Wednesday (13.02%), while Sunday's share dropped to 15.81% from 16.35%, although it still remained the busiest day.

Distribution of DDoS attacks by day of the week, Q2 2022 (download)

Tuesday (14.06%) and Saturday (15.59%) both grew, and Monday (14.22%) dropped. As a result, Saturday and Sunday saw the highest level of DDoS activity.

Duration and types of DDoS attacks

Q2 2022 saw a marked reduction in the share of long (20 hours and longer) attacks in the total DDoS duration, to slightly more than 7% from almost 20% in the first quarter. In quantitative terms, these attacks accounted for just 0.3% of the total, with 0.24% being attacks that lasted 20–49 hours.

Shorter DDoS attacks of up to 4 hours accounted for 74.12% of the total duration and 95.24% of the total number. The share of attacks lasting 5–19 hours remained

virtually unchanged (4.28% of the total against 4.32% in Q1 2022), but the proportion shifted slightly toward attacks 5 to 9 hours long.

The quarter's longest attacks continued for 423 and 403 hours (approximately 17.5 and 17 days), which was 126 hours shorter than the first quarter's record attack of 549 hours (nearly 23 days). The average attack duration dropped from nearly two hours to around 1 hour 45 minutes.

Distribution of DDoS attacks by duration, Q1 and Q2 2022 (download)

The share of UDP flood, the main DDoS technique employed by the botnets that we have observed, rose again in Q2 2022 to 62.53%. SYN flood remained in second place with a 20.25% share. The share of TCP flood shrank to almost half its former size at 11.40%, but this type of flood still kept third place. The share of HTTP flood (2.43%) remained unchanged, whereas GRE flood rose to 3.39%, rising to fourth place.

Distribution of DDoS attacks by type, Q2 2022 (download)

Geographic distribution of botnets

The share of botnet control servers located in the US (46.17%) dropped by 9.3% from Q1 2022, but the country remained the leader. Second came the Netherlands (14.49%), followed by Germany (9.11%), the two countries swapping rankings. The Czech Republic, previously fourth, all but dropped out of the TOP 10, sharing ninth, tenth and eleventh places with Canada and Croatia (1.24%). Russia (4.76%) and France (3.52%) climbed one position each as a result.

Distribution of botnet C2 servers by country, Q2 2022 (download)

Singapore (2.69%) and Vietnam (2.48%) were sixth and seventh, respectively, their shares quadrupling compared to the previous reporting period. The UK (2.07%) dropped to eighth position.

Attacks on IoT honeypots

China (14,22%) remained the leader by number of attacks on Kaspersky SSH honeypots in Q2, although the gap with the US (13.52%) narrowed significantly. Germany (5.64%) and Brazil (5.43%) also kept third and fourth place, respectively, whereas Singapore (4.71%) pushed Hong Kong (4.35%) from fifth place and was closely followed by India (4.70%). South Korea (4.21%) was eighth, Russia (3.41%) was ninth, and the UK (3.33%) rounded out the TOP 10.

Bots from Russia were ahead of other countries and regions by number of attacks at 54.93%. The US was second by number of attacks on SSH honeypots and number of bots associated with these at 7.82%. Vietnam (6.74%) was third: bots located in that country launched more than 1.5 million attacks on our honeypots in Q2 2022. China, which was second in the previous quarter, now slid to fourth place with 4.96%.

Geographic distribution of devices from which attempts were made to attack Kaspersky SSH honeypots, Q2 2022 (download)

The devices that attacked Kaspersky Telnet honeypots in Q2 2022 were mostly located in China, too (39.41% of them). These were also responsible for more than half (58.89%) of all attacks. India was second by bot count (6.90%), but only seventh in terms of bot activity (2.5%). The Netherlands had the second-highest level of bot activity (8.11%). Russia was third on both lists, home to 5.83% of all bots which launched 7.48% of all attacks on the honeypots.

Geographic distribution of devices from which attempts were made to attack Kaspersky Telnet honeypots, Q2 2022 (download)

Conclusion

The second quarter was calmer than the first in terms of DDoS attacks. This is nothing new: we always observe a drop in activity as summer nears. However, the changes in the number of attacks within the quarter did not conform to that trend: botnet activity grew steadily between April and June, following a slump at the end of the previous quarter. This was in line with the crypto collapse, an event that typically gives a boost to DDoS attacks. The attack geography did not change significantly as compared to past reporting periods, but it is worth noting that attacks linked to concurrent geopolitical events may utilize specially created resources not accounted for in our botnet statistics.

Now for our forecasts. Russia's situation is unlikely to change any time soon as long as the political agenda remains the same. DDoS activity in that country has reached a peak of sorts: anyone who is a desirable target or can be attacked is now under attack. We expect similar figures for Russia in Q3 2022 to those in Q2. In view of the cryptocurrency situation, we expect the DDoS market to grow globally. This may have an indirect effect on Russia: the prices of botnet rental will likely drop, making DDoS more affordable as a service, which means the resources that were previously too expensive to attack will now be accessible targets. In particular, one may predict a rise in attacks on educational websites which is already taking shape — although it is hard to say if this is a persistent trend, seasonal variation or an accidental fluctuation. One way or another, the number of DDoS attacks will not dwindle. There are no prerequisites for a lower threat level anywhere in sight, whereas the growth factors are plenty.