DDoS attacks in Q2 2018

News overview

Q2 2018 news includes: non-standard use of old vulnerabilities, new botnets, the cutthroat world of cryptocurrencies, a high-profile DDoS attack (or not) with a political subtext, the slashdot effect, some half-baked attempts at activism, and a handful arrests. But first things first.

Knowing what we know about the devastating consequences of DDoS attacks, we are not inclined to celebrate when our predictions come true. Alas, our forecast in the previous quarter's report was confirmed: cybercriminals continue to seek out new non-standard amplification methods. Even before the panic over the recent wave of Memcached-based attacks had subsided, experts discovered an amplification method using another vulnerability—in the Universal Plug and Play protocol, known since 2001. It allows garbage traffic to be sent from several ports instead of just one, switching them randomly, which hinders the blocking process. Experts reported two attacks (April 11 and 26) in which this method was likely used; in the first instance, the DNS attack was amplified through UPnP, and in the second the same was applied to an NTP attack. In addition, the Kaspersky DDoS Protection team observed an attack that exploited a vulnerability in the CHARGEN protocol. A slightly weaker attack using the same protocol to amplify the flood (among other methods) targeted the provider ProtonMail, the reason for which was an unflattering comment made by the company's executive director.

New botnets are causing more headaches for cybersecurity specialists. A noteworthy case is the creation of a botnet formed from 50,000 surveillance cameras in Japan. And a serious danger is posed by a new strain of the Hide-n-Seekmalware, which was the first of all known bots to withstand, under certain circumstances, a reboot of the device on which it had set up shop. True, this botnet has not yet been used to carry out DDoS attacks, but experts do not rule out such functionality being added at a later stage, since the options for monetizing the botnet are not that many.

One of the most popular monetization methods remains attacking cryptocurrency sites and exchanges. What's more, DDoS attacks are used not only to prevent competitors from increasing their investors, but as a way of making a big scoop. The incident with the cryptocurrency Verge is a case in point: in late May, a hacker attacked Verge mining pools, and made off with XVG 35 million ($1.7 million). In the space of two months, the currency was hacked twice, although the preceding attack was not a DDoS.

Not only that, June 5 saw cybercriminals bring down the Bitfinex cryptocurrency exchange, with the system crash followed by a wave of garbage traffic, pointing to a multistage attack that was likely intended to undermine credibility in the site. It was probably competitive rivalry that caused the renowned online poker site, Americas Cardroom, to suffer a DDoS attack that forced first the interruption and then cancellation of a tournament. That said, it was rumored that the attack could have been a political protest against the in-game availability of Donald Trump and Kim Jong Un avatars.

As always, the most media hype in the past quarter was generated by politically motivated DDoS attacks. In mid-April, British and US law enforcement bodies warned that a significant number of devices had been seized by Russian (supposedly Kremlin-sponsored) hackers in the US, the EU, and Australia with a view to carrying out future attacks. Then just a few days later, in late April, it was a Russian target that got hit: the site of the largest Russian political party, United Russia, was downfor two whole days, yet there was precious little public speculation about the masterminds behind the DDoS campaign.

An attack on the Danish railway company DSB, which struggled to serve passengers for several days as a result, was also alleged to be politically motivated. Some see it as a continuation of the attack on Swedish infrastructure last fall.

At the end of the quarter, attention was focused on the Mexican elections and an attack on an opposition party website hosting materials about the illegal activities of a rival. According to the victim, the attack began during a pre-election debate when the party's candidate showed viewers a poster with the website address. However, it was immediately rumored that DDoS was not the culprit, but the Slashdot effect, which Reddit users also call "the hug of death." This phenomenon has been around since the dawn of the Internet, when bandwidth was a major issue. But it's still encountered to this day when a small resource suffers a major influx of legitimate web traffic on the back of media hype.

The Slashdot effect was also observed by the Kaspersky DDoS Protection team in early summer. After a press conference by the Russian president, a major news outlet covering the event experienced a powerful wave of tens of thousands of HTTP GET requests all sent simultaneously. The size of the supposed botnet suggested a new round of attacks involving IoT devices, but further analysis by KDP experts showed that all suspicious queries in the User Agent HTTP header contained the substring "XiaoMi MiuiBrowser". In fact, owners of Xiaomi phones with the browser app installed received a push notification about the outcome of the conference, and it seems that many took an interest and followed the link, causing a glut of requests.

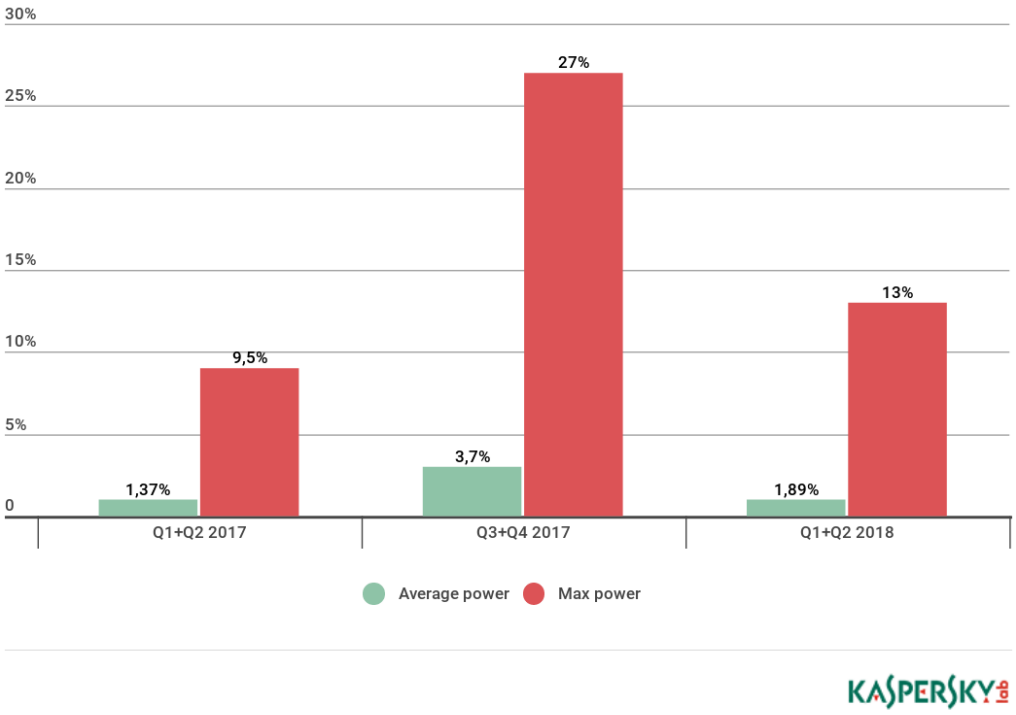
Meanwhile, law enforcement agencies have been making every effort to prevent organized attacks: in late April, Europol managed to shut down Webstresser.org, the world's largest DDoS-for-hire service. When it was finally blocked, the portal had more than 136,000 users and had served as the source of more than 4 million DDoS attacks in recent years. After the fall of Webstresser, conflicting trends were reported: some companies observed a significant decline in DDoS activity in Europe (although they warned that the drop was going to be relatively short-lived); others, however, pointed to a rise in the number of attacks across all regions, which may have been the result of attackers seeking to compensate by creating new botnets and expanding old ones.

On top of that, several DDoS attack masterminds were caught and convicted. German hacker ZZboot was sentenced for attacking major German and British firms with ransom demands. However, he avoided jail time, receiving 22 months of probation. At the other end of the Eurasian continent, in Taipei, a hacker named Chung was arrested for allegedly attacking the Taiwan Bureau of Investigation, the Presidential Administration, Chungwa Telecom, and the Central Bank. In the other direction, across the pond, a self-proclaimed hacktivist was arrested in the US for obstructing the work of police in Ohio.

Another, less significant, but more curious arrest took place in the US: an amateur hacker from Arizona was arrested, fined, and jailed after an online acquaintance posted a tweet with his name. Despite his rudimentary skills, the cybercriminal, calling himself the "Bitcoin Baron," had terrorized US towns for several years, crashing the websites of official institutions and demanding ransoms; in one incident, his actions seriously hindered emergency response services. He too tried to position himself as a cyberactivist, but his bad behavior ruined any reputation he might have had, especially his alleged (only by himself, it should be said) attempt to bring down the site of a children's hospital by flooding it with child pornography.

Quarter trends

In H1 2018, the average and maximum attack power fell significantly compared to H2 2017. This can be explained by the seasonal slowdown that is usually observed at the start of the year. However, a comparison of H1 indicators for 2017 and 2018 shows a measurable rise in attack power since last year.



Change in DDoS attack power, 2017-2018

One way to increase the attack power is third-party amplification. As mentioned in the news overview, hackers continue to look for ways to amplify DDoS attacks through new (or well-forgotten old) vulnerabilities in widely popular software, not without success, unfortunately. This time, the KDP team detected and repelled an attack with a capacity in the tens of Gbit/s that exploited a vulnerability in the CHARGEN protocol—an old and very simple protocol described in RFC 864 way back in 1983.

CHARGEN was intended for testing and measurement purposes, and can listen on both the TCP and UDP sockets. In UDP mode, the CHARGEN server responds to any request with a packet with a string length from 0 to 512 random ASCII characters. Attackers use this mechanism to send requests to the vulnerable CHARGEN server, where the outgoing address is substituted by the address of the victim. US-CERT estimates the amplification factor at 358.8x, but this figure is somewhat arbitrary, since the responses are generated randomly.

Despite the protocol's age and limited scope, many open CHARGEN servers can be found on the Internet. They are mainly printers and copying devices in which the network service is enabled by default in the software.

The use of CHARGEN in UDP attacks, as reported by KDP and other providers (Radware, Nexusguard), may indicate that attacks using more convenient protocols (for example, DNS or NTP) are becoming less effective, since there exist well-developed methods to combat this kind of UDP flooding. But the simplicity of such attacks makes cybercriminals unwilling to abandon them; instead they hope that modern security systems will not be able to resist antiquated methods. And although the search for non-standard holes will doubtless continue, CHARGEN-type amplification attacks are unlikely to take the world by storm, since vulnerable servers lack a source of replenishment (how often are old copiers connected to the Internet?).

If cybercriminals are going retro in terms of methods, when it comes to targets they are breaking new ground. DDoS attacks against home users are simple, but not profitable, whereas attacks on corporations are profitable, but complex. Now DDoS planners have found a way to get the best of both worlds—in the shape of the online games industry and streamers. Let's take as an example

the growing popularity of e-sports tournaments, in which the victors walk away with tens—sometimes hundreds—of thousands of dollars. The largest events are usually held at special venues with specially setup screens and stands for spectators, but the qualifying rounds to get there often involve playing from home. In this case, a well-planned DDoS attack against a team can easily knock it out of the tournament at an early stage. The tournament server might also be targeted, and the threat of disruption could persuade the competition organizers to pay the ransom. According to Kaspersky Lab client data, DDoS attacks on e-sports players and sites with the goal of denying access are becoming increasingly common.

Similarly, cybercriminals are trying to monetize the market of video game streaming channels. Streaming pros show live playthroughs of popular games, and viewers donate small sums to support them. Naturally, the larger the audience, the more money the streamer gets for each broadcast; top players can earn hundreds or thousands of dollars, which basically makes it their job. Competition in this segment is fierce and made worse by DDoS attacks with the capacity to interfere with livestreams, causing subscribers to look for alternatives.

Like e-sports players, home streamers have virtually no means of protection against DDoS attacks. They are essentially reliant on their Internet provider. The only solution at present could be to set up specialized platforms offering greater protection.

Methodology

Kaspersky Lab has extensive experience of combating cyber threats, including DDoS attacks of all types and complexity. Company experts monitor the actions of botnets using the Kaspersky DDoS Intelligence system.

The DDoS Intelligence system is part of the Kaspersky DDoS Protection solution, and intercepts and analyzes commands sent to bots from C&C servers. What's more, the system is proactive, not reactive—there's no need to wait for a user device to get infected or a command to be executed.

This report contains DDoS Intelligence statistics for Q2 2018.

In the context of this report, it is assumed that an incident is a separate (single) DDoS-attack 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 incident 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 Lab. Note that botnets are just one of the tools for performing DDoS attacks, and that the data presented in this report do not cover every single DDoS attack that occurred during the period under review.

Quarter results

- The stormiest period for DDoS attacks was the start of the quarter, particularly mid-April. By contrast, late May and early June were fairly quiet.

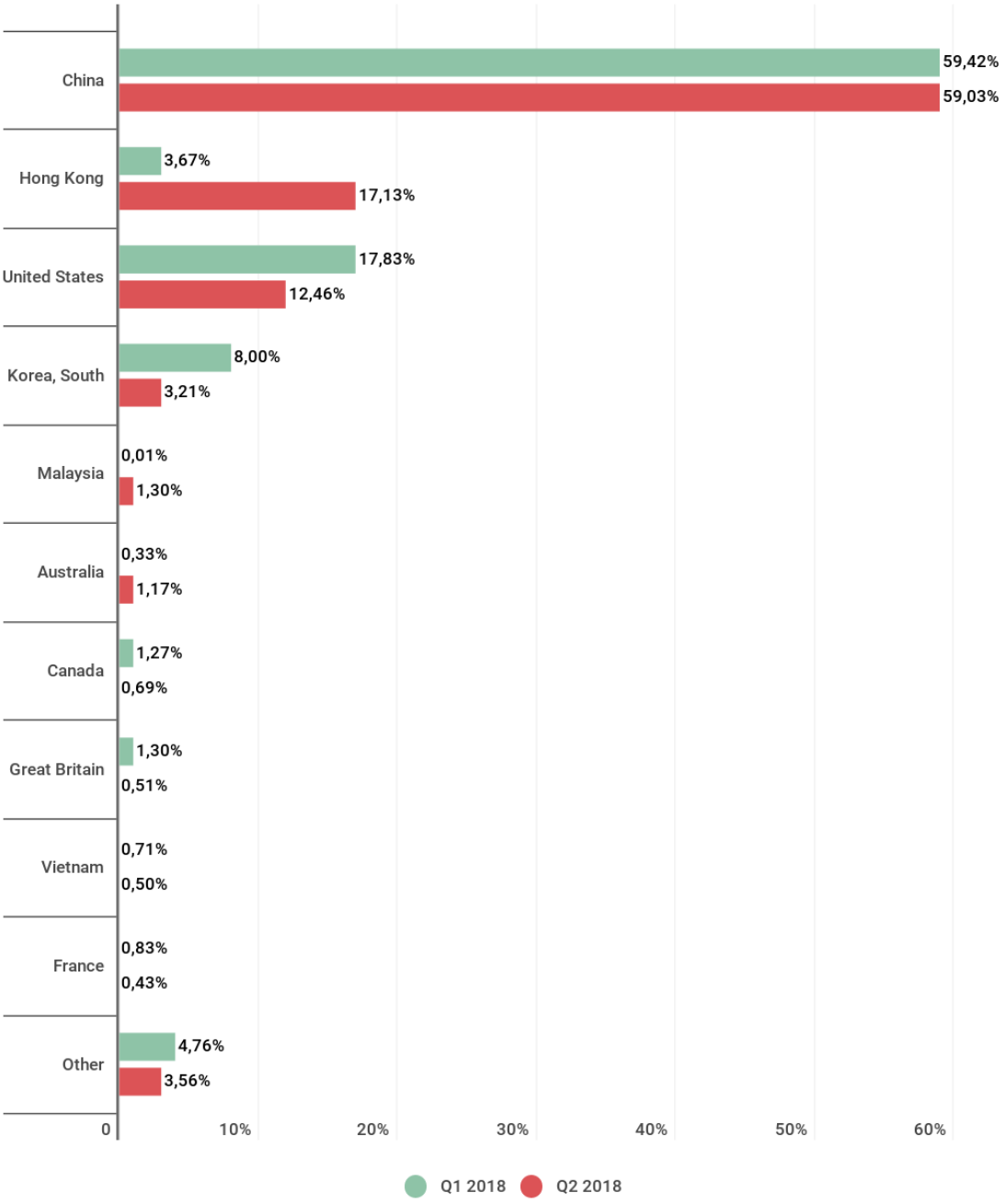
- Top spot in terms of number of attacks was retained by China (59.03%), with Hong Kong (17.13%) in second. It also entered the Top 3 by number of unique targets with 12.88%, behind only China (52.36%) and the US (17.75%).
- The attacks were quite evenly distributed across the days of the week. The most and least popular were Tuesday and Thursday, respectively, but the difference is slight.
- The share of SYN attacks rose sharply to 80.2%; second place went to UDP attacks with 10.6%.
- The share of attacks from Linux botnets increased significantly to 94.47% of all single-family attacks.

Geography of attacks

The latest quarter threw up a number of surprises. The leader by number of attacks is still China, with its share practically unchanged (59.03% against 59.42% in Q1). However, for the first time since monitoring began, Hong Kong broke into the Top 3, rising from fourth to second: its share increased almost fivefold, from 3.67% to 17.13%, squeezing out the US (12.46%) and South Korea (3.21%), whose shares declined by roughly 5 p.p. each.

Another surprise package in the territorial ranking was Malaysia, which shot up to fifth place, now accounting for 1.30% of all DDoS attacks. It was joined in the Top 10 by Australia (1.17%) and Vietnam (0.50%), while the big-hitters Japan, Germany, and Russia all dropped out. Britain (0.50%) and Canada (0.69%) moved into eighth and seventh, respectively.

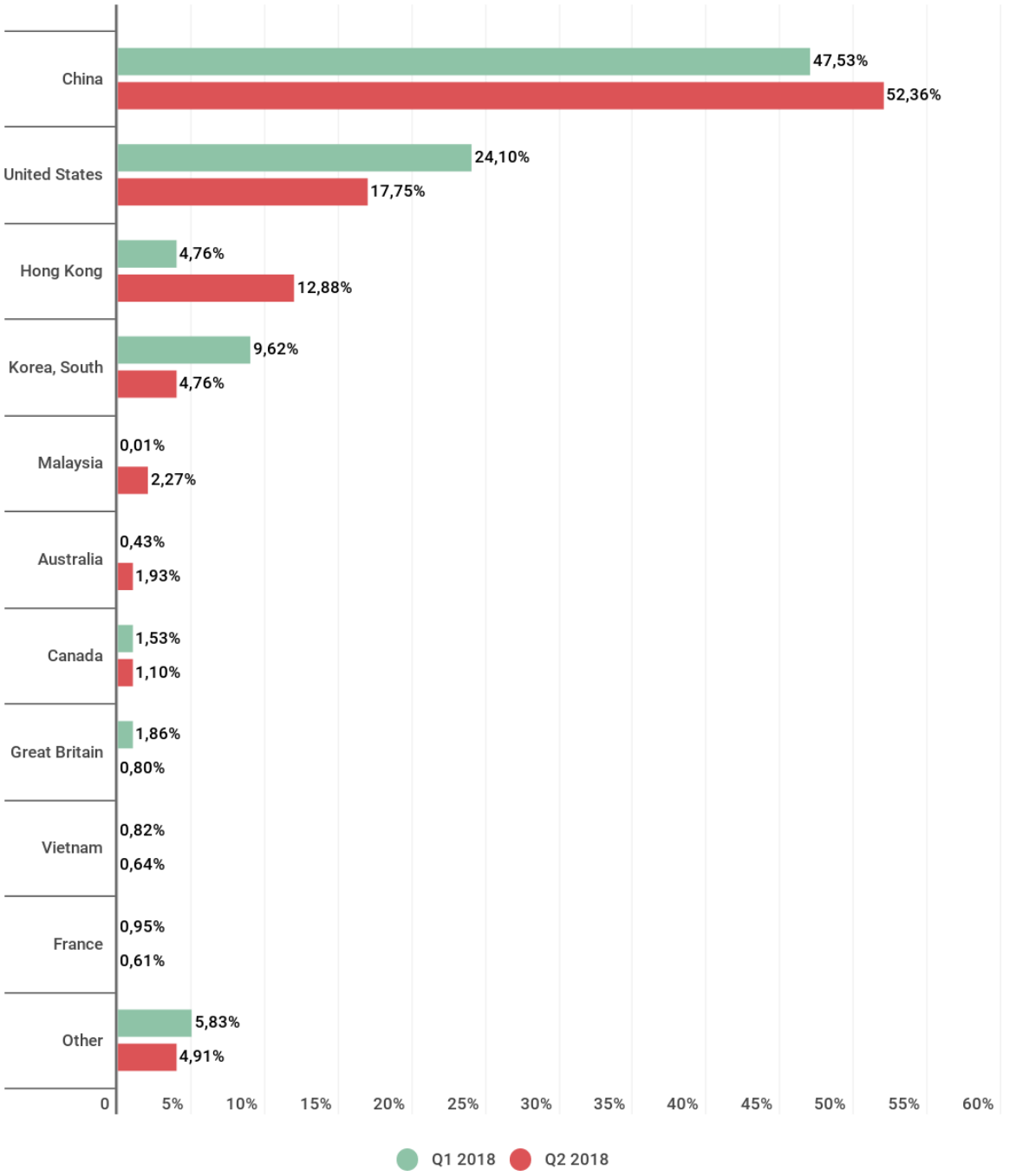
The Top 10 in Q2 also had a greater share of the total number of attacks than in Q1: 96.44% compared with 95.44%.



Distribution of DDoS attacks by country, Q1 and Q2 2018

The territorial distribution of unique targets roughly corresponds to the distribution of the number of attacks: China has the largest share (52.36%), a rise of 5 p.p. against the previous quarter. Second place belongs to the US (17.5%) and third to Hong Kong (12.88%), up from fourth, replacing South Korea (4.76%) (note that in Hong Kong the most popular targets are now Microsoft Azure servers). Britain fell from fourth to eighth, now accounting for 0.8% of unique targets.

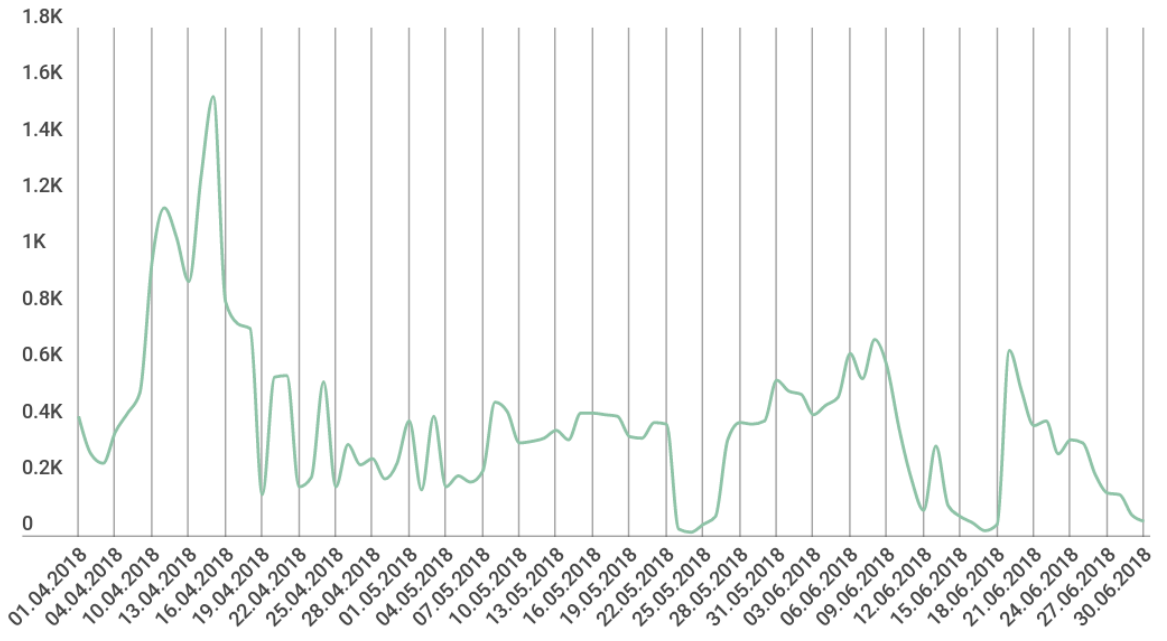
The Top 10 said goodbye to Japan and Germany, but welcomed Malaysia (2.27%) in fourth place and Australia (1.93%) just behind in fifth. This quarter's Top 10 accounted for slightly more of the total number of unique attacks, reaching 95.09% against 94.17% in Q1.



Distribution of unique DDoS-attack targets by country, Q1 and Q2 2018

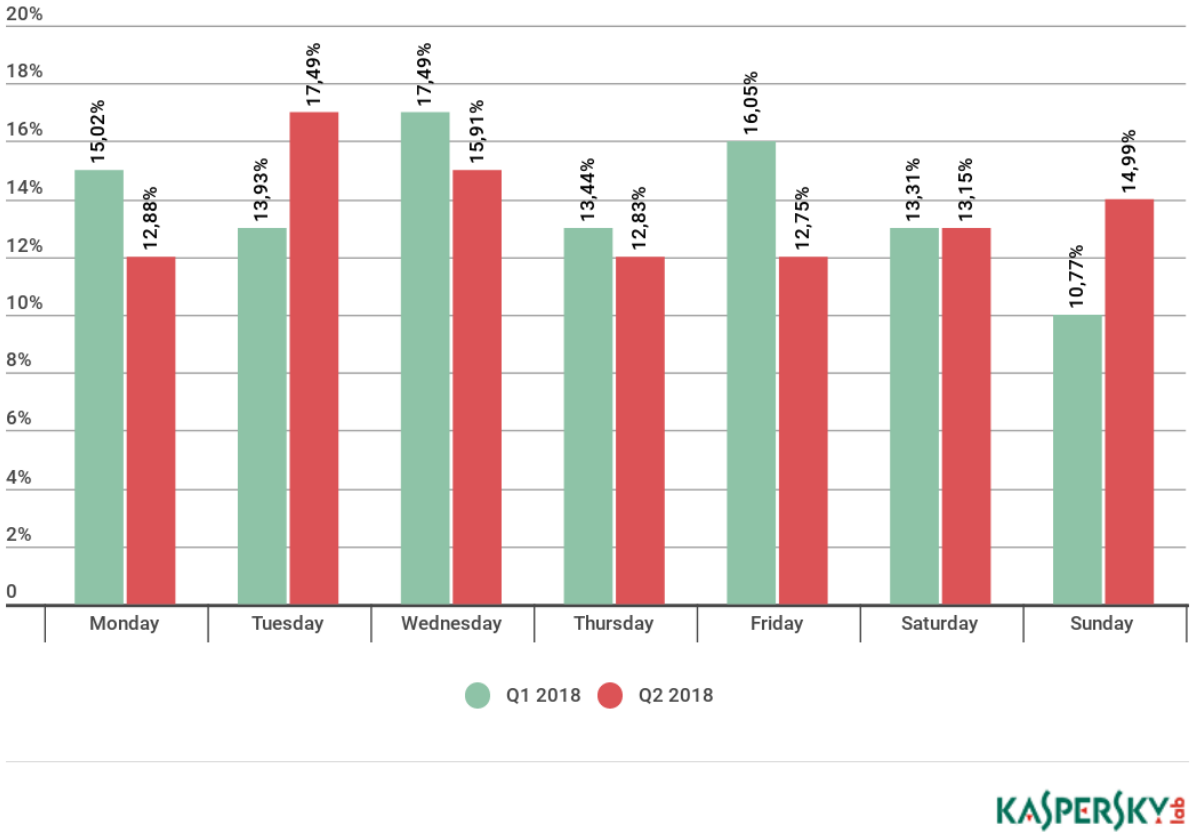
Dynamics of the number of DDoS attacks

Peak activity in Q2 2018 was observed in mid-April: a significant increase in the number of attacks was registered in the middle third of this month, with two large spikes occurring just days apart: April 11 (1163) and April 15 (1555). The quarter's deepest troughs came in the second half and at the end: the calmest days were May 24 (13) and June 17 (16).



Dynamics of the number of DDoS attacks, Q2 2018

In Q2 2018, Sunday went from being the quietest day for cybercriminals to the second most active: it accounted for 14.99% of attacks, up from 10.77% in the previous quarter. But gold in terms of number of attacks went to Tuesday, which braved 17.49% of them. Thursday, meanwhile, went in the opposite direction: only 12.75% of attacks were logged on this day. Overall, as can be seen from the graph, in the period April-June the attack distribution over the days of the week was more even than at the beginning of the year.

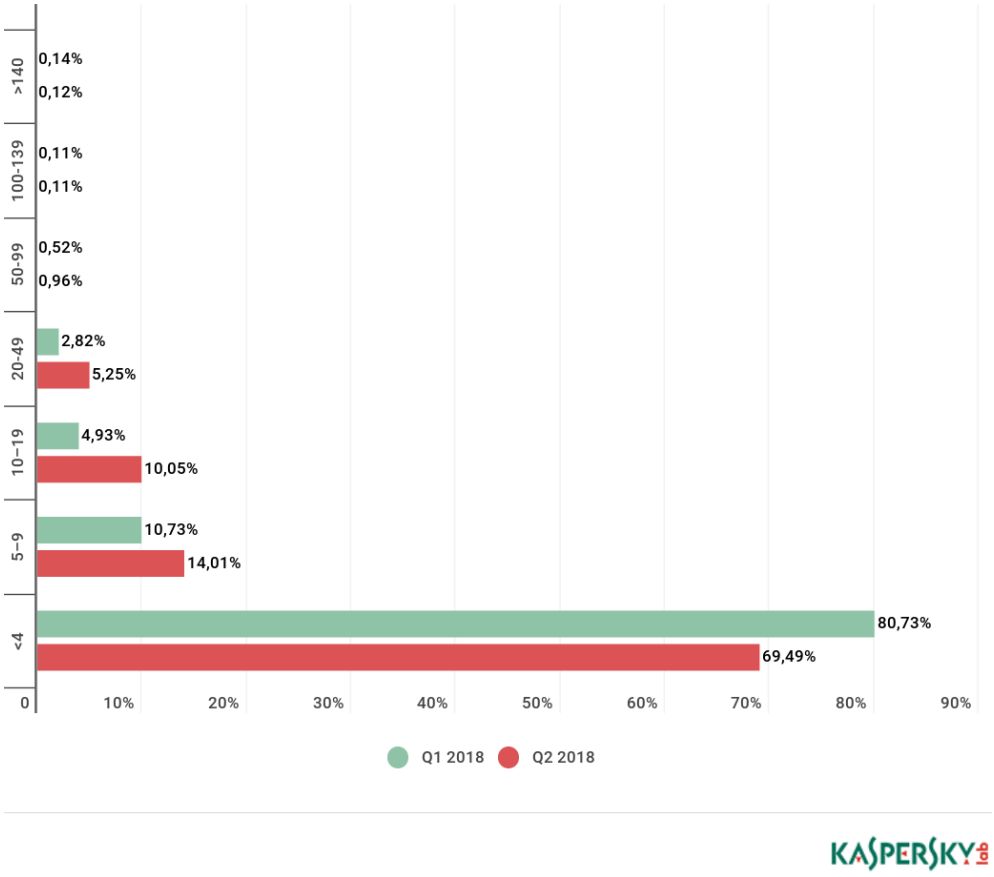


Distribution of DDoS attacks by day of the week, Q1 and Q2 2018

Duration and types of DDoS attacks

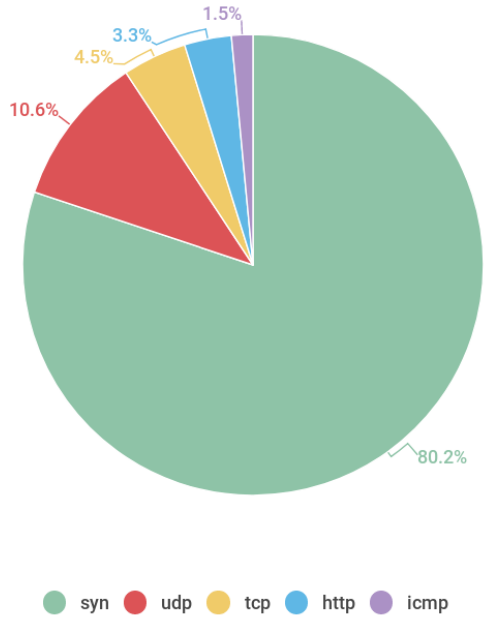
The longest attack in Q2 lasted 258 hours (almost 11 days), slightly short of the previous quarter's record of 297 hours (12.4 days). This time, the focus of persevering hackers was an IP address belonging to China Telecom.

Overall, the share of long-duration attacks fell by 0.02 p.p. to 0.12%. Whereas the share of attacks lasting from 100 to 139 hours remained the same, the share of attacks from 10 to 50 hours almost doubled (from 8.28% to 16.27%); meanwhile, the share of attacks lasting from five to nine hours increased nearly by half (from 10.73% to 14.01%). The share of short-duration attacks (up to four hours) fell sharply from 80.73% in January to 69.49% in March.



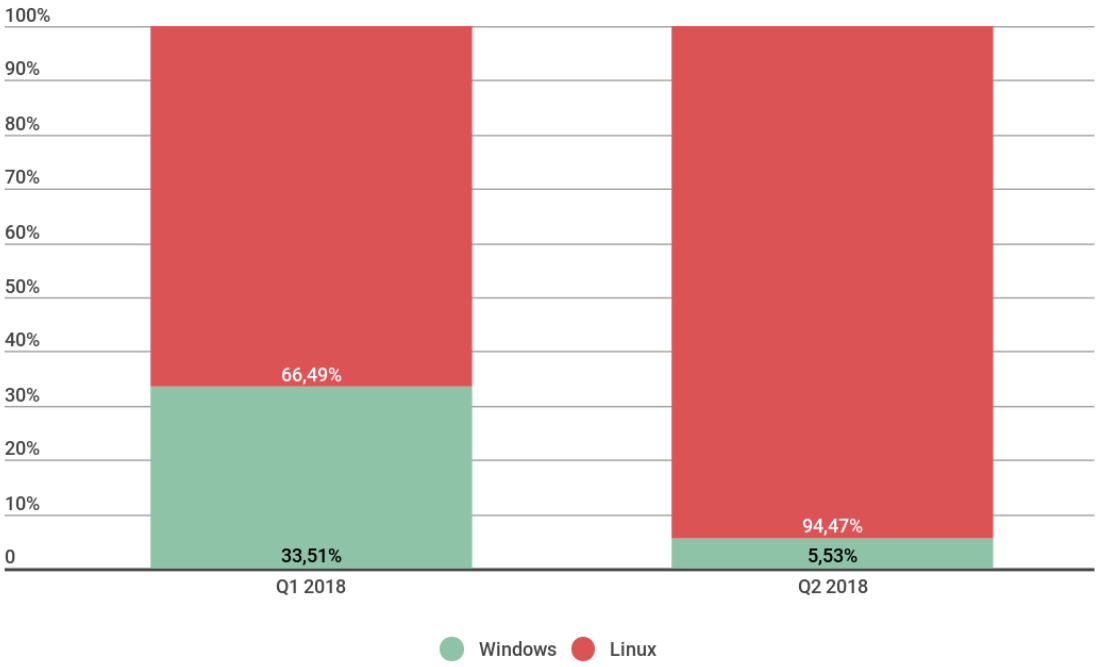
Distribution of DDoS attacks by duration (hours), Q1 and Q2 2018

All other types of attacks decreased in share; UDP attacks are in second place (10.6%), while TCP, HTTP, and ICMP constitute a relatively small proportion.



KASPERSKY lab

Distribution of DDoS attacks by type, Q2 2018

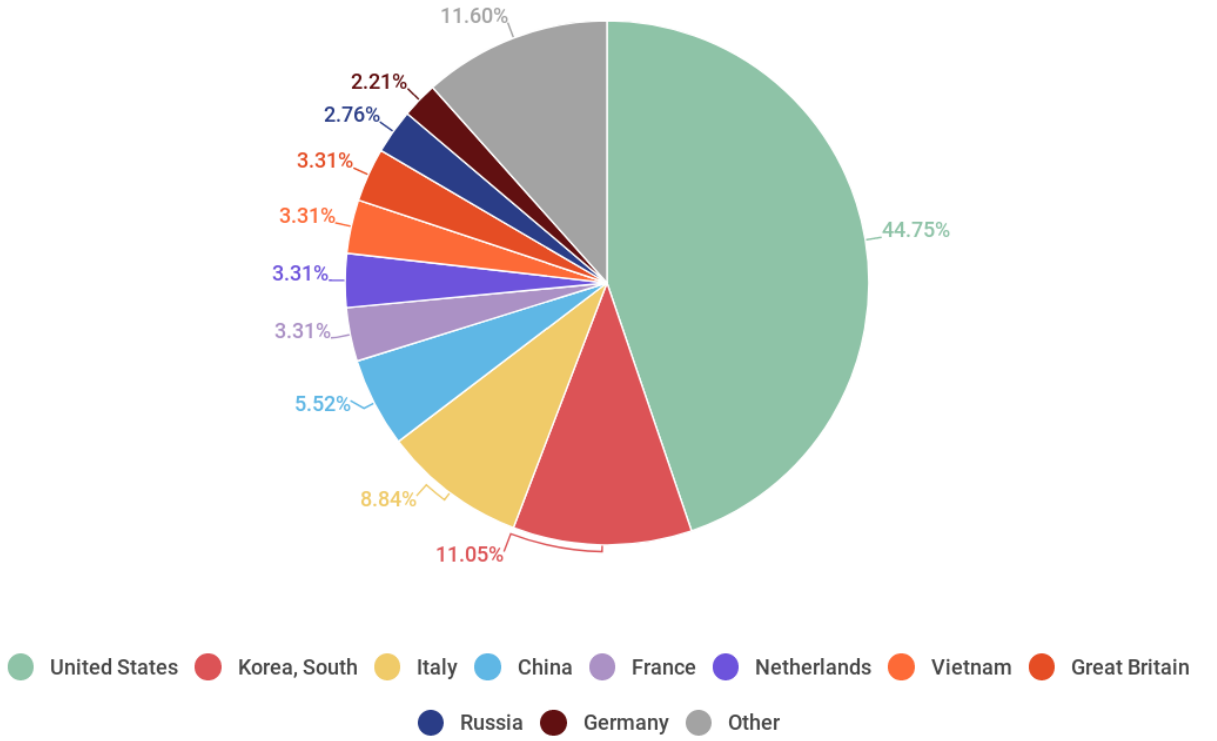


KASPERSKY lab

Correlation between Windows- and Linux-based botnet attacks, Q2 2018

Geographical distribution of botnets

The Top 10 regions by number of botnet C&C servers underwent some significant changes. Top spot went to the US with almost half of all C&C centers (44.75% against 29.32% in Q1). South Korea (11.05%) sank from first to second, losing nearly 20 p.p. China also dropped significantly (from 8.0% to 5.52%). Its place was taken by Italy, whose share climbed from 6.83% in the previous quarter to 8.84%. The Top 10 saw the departure of Hong Kong, but was joined—for the first time since our records began—by Vietnam, whose 3.31% was good enough for seventh place.



Distribution of botnet C&C servers by country, Q2 2018

Conclusion

In Q2 2018, cybercriminals continued the above-outlined trend of searching for exotic holes in UDP transport protocols. It surely won't be long before we hear about other sophisticated methods of attack amplification.

Another technical discovery of note is the potential for creating botnets using the UPnP protocol; although evidence for them exists, they are still extremely rare in the wild, fortunately.

Windows botnet activity decreased: in particular, Yoyo activity experienced a multifold drop, and Nitol, Drive, and Skill also declined. Meanwhile, Xor for Linux significantly increased its number of attacks, while another infamous Linux botnet, Darkai, scaled back slightly. As a result, the most popular type of attack was SYN flooding.

The total attack duration changed little since the previous quarter, but the share of medium-duration attacks increased, while the share of shorter ones decreased. The intensity of attacks also continues to grow. The most lucrative targets for cybercriminals seem to be cryptocurrencies, but we can soon expect to see high-profile attacks against e-sports tournaments as well as relatively small ransoms targeting individual streamers and players. Accordingly, there will be market demand for affordable individual anti-DDoS protection.