News Overview

Thanks to IoT botnets, DDoS attacks have finally turned from something of a novelty into an everyday occurrence. According to the A10 Networks survey, this year the 'DDoS of Things' (DoT) has reached critical mass – in each attack, hundreds of thousands of devices connected to the Internet are being leveraged.

The fight against this phenomenon is just beginning – IoT equipment vendors are extremely slow to strengthen information security measures in their own products. However, certain successes have been achieved in combating attackers behind the DDoS of Things. The well-known info security journalist Brian Krebs managed to identify the author of the infamous IoT malware Mirai. In the UK, the author of an attack on Deutsche Telekom was arrested. According to the charges, he allegedly assembled an IoT botnet from routers in order to sell access to it. He faces up to 10 years in prison in Germany.

Cheaper DoS tools and a growth in their number has caused an inevitable increase in the number of attacks on notable resources. For instance, unknown attackers took down the site of the Austrian Parliament, as well as more than a hundred government servers in Luxembourg. No one took responsibility for the attacks and no demands were made, which may mean the attacks were a test run, or simply hooliganism.

Plans by supporters of the Democratic Party to launch a massive attack on the White House site as a protest against the election of Donald Trump the US president came to nothing – there were no reports of problems with the site. Nevertheless, DDoS attacks have taken root in the US as a type of political protest. Two weeks before the inauguration, the conservative news site Drudge Report, which actively supported Trump during the election campaign, was attacked.

Law enforcement agencies took notice of this alarming trend, and the US Department of Homeland Security eventually stepped in to provide protection from DDoS attacks. The Department declared it aimed to "build effective and easily implemented network defenses and promote adoption of best practices by the private sector" in order "to bring about an end to the scourge of DDoS attacks."

However, the main goal of the DDoS authors is still to make money. In this respect, banks and broker companies remain the most attractive targets. DDoS attacks are capable of causing such serious material and reputational damage that many organizations prefer to pay the cybercriminals' ransom demands.

Trends of the quarter

There's usually a distinct lull in DDoS attacks at the beginning of the year. This may be due to the fact that the people behind these attacks are on vacation, or perhaps there's less demand from their customers. In any case, this trend has been observed for the last five

years – Q1 is off season. The first quarter of this year was no exception: Kaspersky Lab's DDoS prevention group recorded very low attack activity. This was in stark contrast to the fourth quarter of 2016. However, despite the now habitual downturn, Q1 of 2017 saw more attacks than the first quarter of 2016, which confirms the conclusion that the overall number of DDoS attacks is growing.

Due to the traditional Q1 lull, it's too early to talk about any trends for 2017; however, a few interesting features are already noticeable:

1. 1. Over the reporting period, not a single amplification-type attack was registered, although attacks to overload a channel without amplification (using a spoofed IP address) were in constant use. We can assume that amplification attacks are no longer effective and are gradually becoming a thing of the past.

2. 2. The number of encryption-based attacks has increased, which is in line with last year's forecasts and current trends. However, this growth cannot as yet be called significant.

As we predicted, complex attacks (application-level attacks, HTTPS) are gaining in popularity. One example was the combined attack (SYN + TCP Connect + HTTP-flood + UDP flood) on the Moscow stock exchange. A distinct feature of this attack was its rare multi-vector nature in combination with relatively low power (3 Gbps). To combat such attacks, it's necessary to use the latest complex protection mechanisms.

Yet another unusual attack affected the site of the Portuguese police force. A notable feature of this attack was the use of vulnerabilities in reverse proxy servers to generate attack traffic. We assume the cybercriminals were trying to disguise the real source of the attack; and to generate traffic, new types of botnets were used, consisting of vulnerable reverse proxies.

On the whole, Q1 2017 didn't bring any surprises. In the second quarter, we expect to see a gradual increase in the proportion of distributed attacks. Based on the next quarter's results, it may be possible to get an idea of what we will face in 2017. For now, we can only guess.

Statistics for botnet-assisted DDoS attacks

Methodology

Kaspersky Lab has extensive experience of combating cyber threats, including DDoS attacks of various types and complexity. The company's experts monitor botnet activity with the help of the DDoS Intelligence system. DDoS Intelligence (part of Kaspersky DDoS Protection) is designed to intercept and analyze commands sent to bots from command and control (C&C) servers, and does not have to wait until user devices are infected or cybercriminal commands are executed in order to gather data.

This report contains the DDoS Intelligence statistics for the first quarter of 2017.

In the context of this report, a single (separate) DDoS attack is defined as an incident during which any break in botnet activity lasts less than 24 hours. If the same web resource was attacked by the same botnet after a break of more than 24 hours, this is regarded as a separate DDoS attack. Attacks on the same web resource from two different botnets are also regarded as separate attacks.

The geographic distribution of DDoS victims and C&C servers is determined according to their IP addresses. In this report, the number of DDoS targets is calculated based on the number of unique IP addresses reported in the quarterly statistics.

It is important to note that DDoS Intelligence statistics are limited to those botnets detected and analyzed by Kaspersky Lab. It should also be noted that botnets are just one of the tools used to carry out DDoS attacks; therefore, the data presented in this report does not cover every DDoS attack that has occurred within the specified time period.

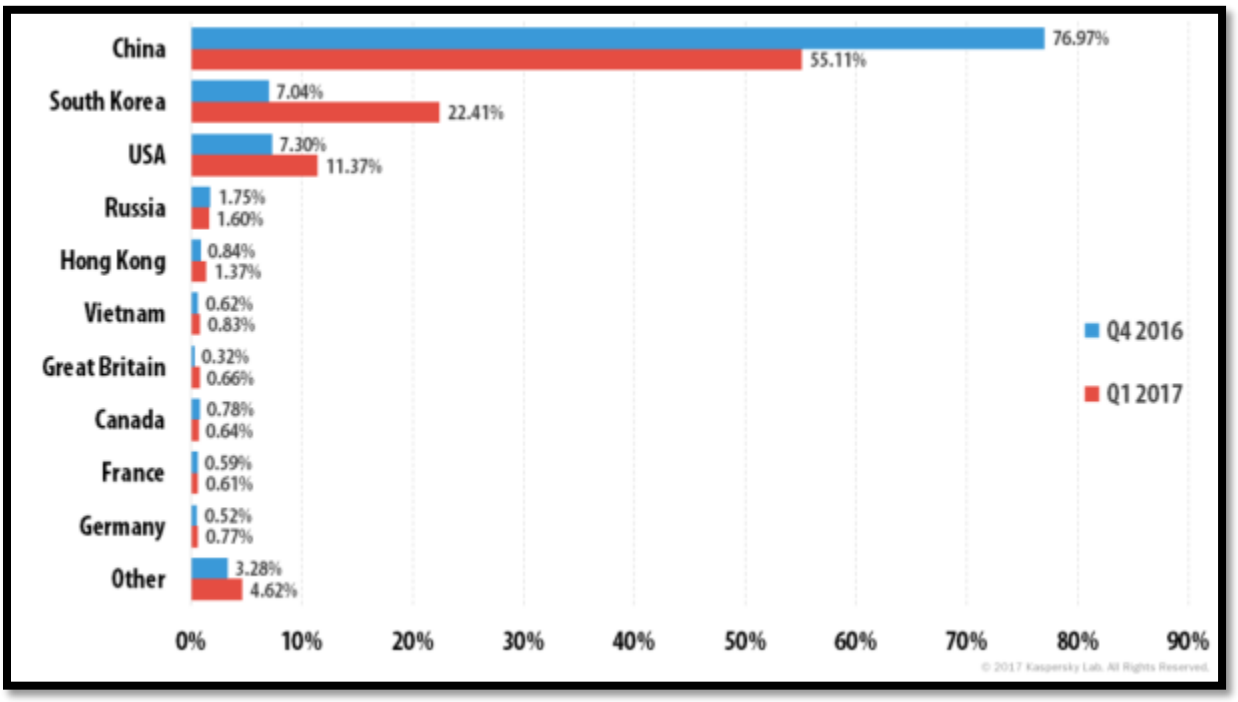
Q1 Summary

- Resources in 72 countries (vs. 80 in Q4 2016) were targeted by DDoS attacks in Q1 2017.
- 47.78% of targeted resources were located in China which is significantly lower than the previous quarter (71.60%).
- China, South Korea and the US remained leaders in terms of both number of DDoS attacks and number of targets, while the Netherlands replaced China in terms of number of detected servers.
- The longest DDoS attack in Q1 2017 lasted for 120 hours – 59% shorter than the previous quarter's maximum (292 hours). A total of 99.8% of attacks lasted less than 50 hours.
- The proportion of attacks using TCP, UDP and ICMP grew considerably, while the share of SYN DDoS declined from 75.3% in Q4 2016 to 48% in the first quarter of 2017.
- For the first time in a year, activity by Windows-based botnets has exceeded that of Linux botnets, with their share increasing from 25% last quarter to 59.8% in Q1 2017.

Geography of attacks

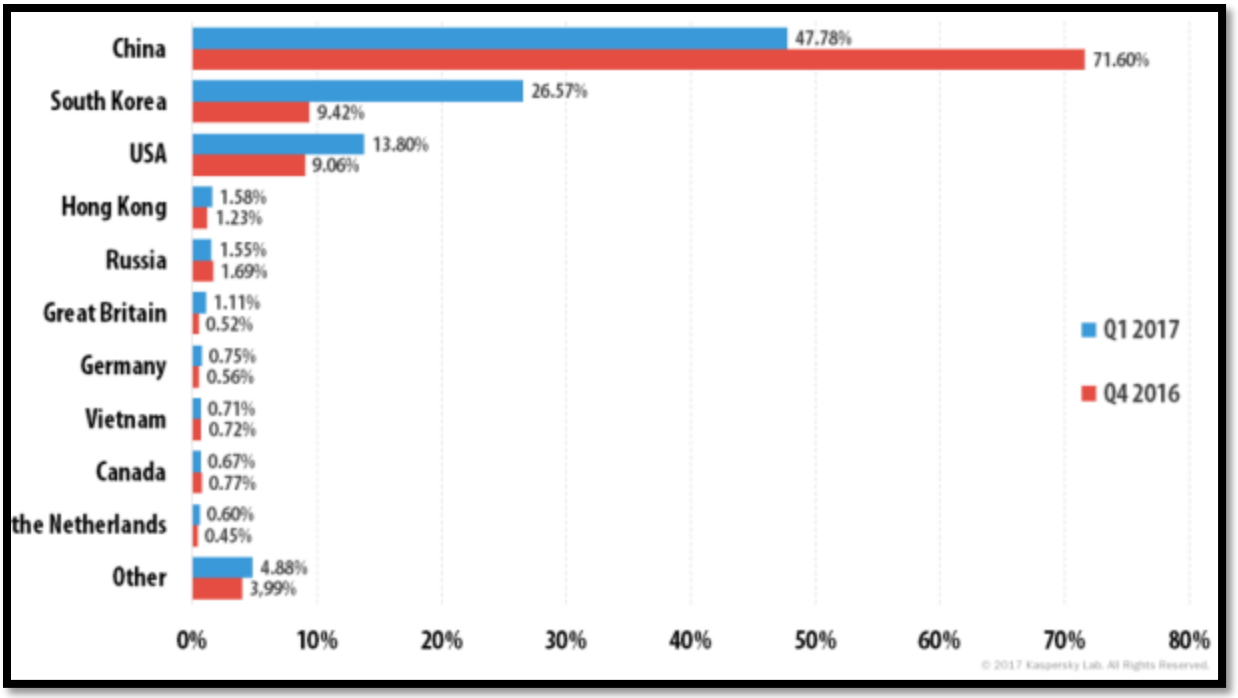
In Q1 2017, the geography of DDoS attacks narrowed to 72 countries, with China accounting for 55.11% (21.9 p.p. less than the previous quarter). South Korea (22.41% vs. 7.04% in Q4 2016) and the US (11.37% vs. 7.30%) were second and third respectively.

The Top 10 most targeted countries accounted for 95.5% of all attacks. The UK (0.8%) appeared in the ranking, replacing Japan. Vietnam (0.8%, + 0.2 p.p.) moved up from seventh to sixth, while Canada (0.7%) dropped to eighth.



Distribution of DDoS attacks by country, Q4 2016 vs. Q1 2017

Statistics for the first quarter show that the 10 most targeted countries accounted for 95.1% of all DDoS attacks.



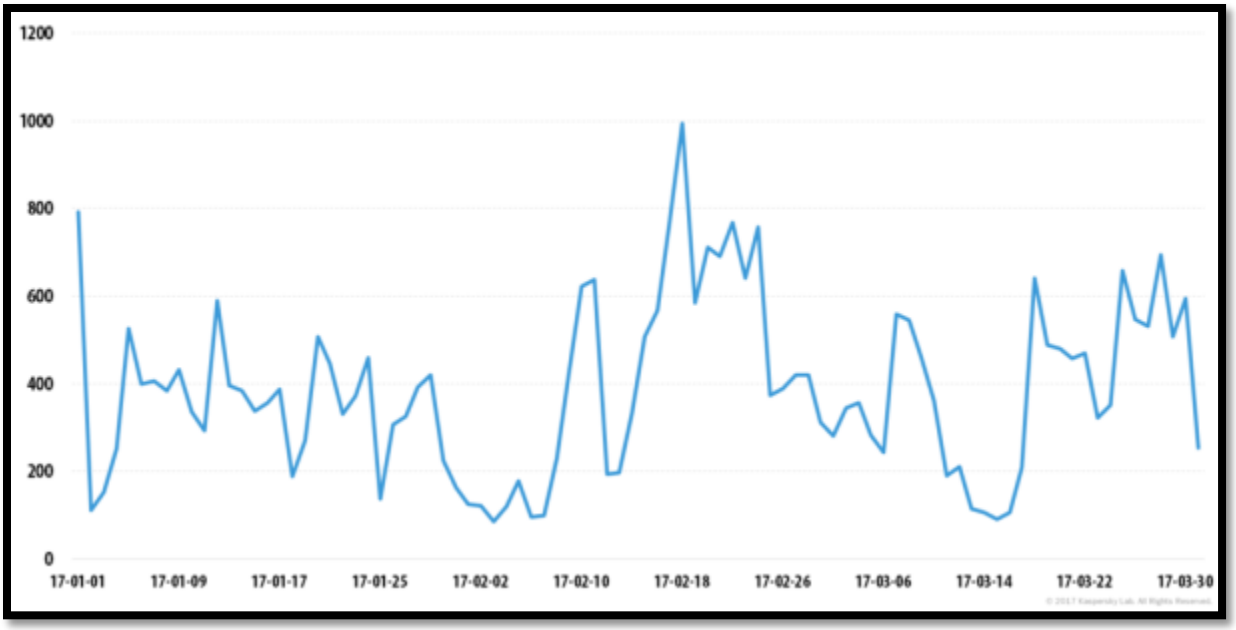
Distribution of unique DDoS attack targets by country, Q4 2016 vs. Q1 2017

Similar to the ranking for attack numbers, targets in China received much less attention from cybercriminals in Q1 2017 – they accounted for 47.78% of attacks, although China still remained the leader in this respect. In fact, the top three remained unchanged from the previous quarter despite dramatic growth in South Korea's share (from 9.42% to 26.57%) and that of the US (from 9.06% to 13.80%).

Russia (1.55%) fell from fourth to fifth place, after its share fell by just 0.14 p.p. Hong Kong took its place (+ 0.35 p.p.). Japan and France were replaced in the Top 10 by the Netherlands (0.60%) and the UK (1.11%).

Changes in DDoS attack numbers

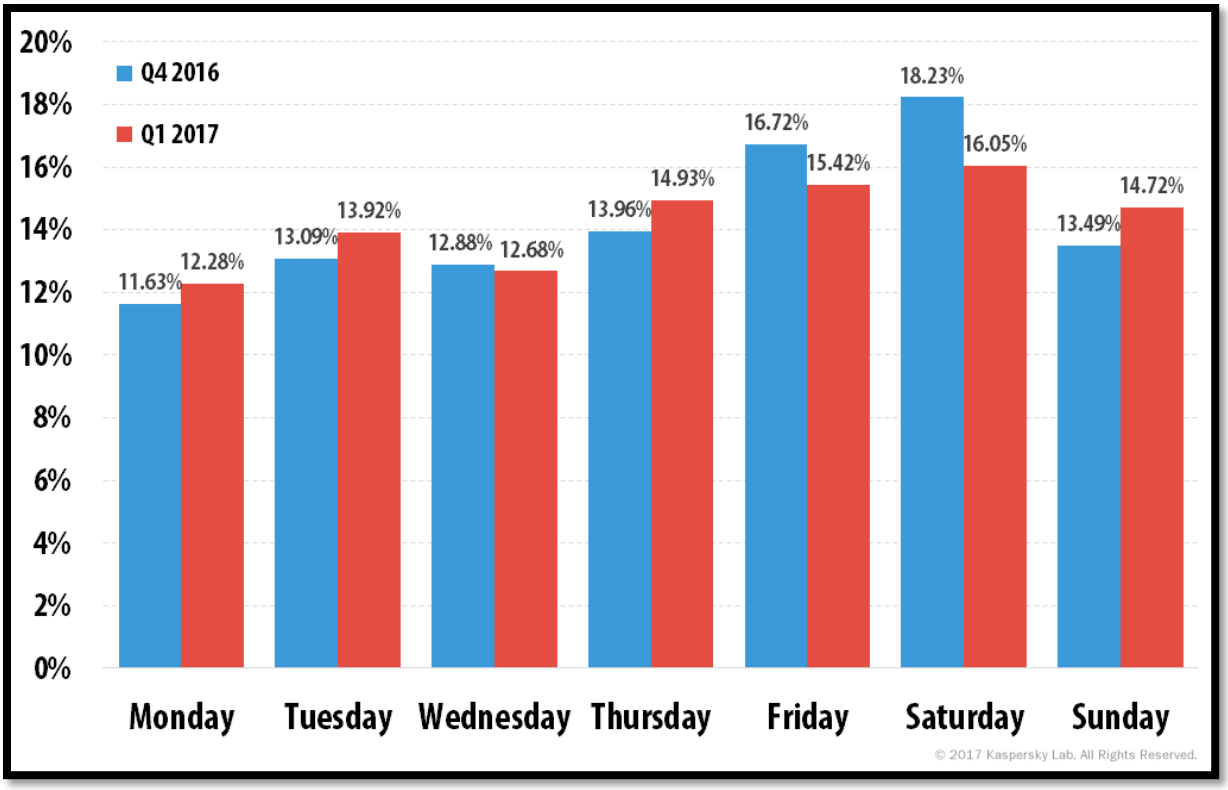
In Q1 2017, the number of attacks per day ranged from 86 to 994. Most attacks occurred on 1 January (793 attacks), 18 February (994) and 20 February (771). The quietest days of Q1 were 3 February (86 attacks), 6 February (95), 7 February (96) and 15 March (91). The overall decline in the number of attacks from the end of January to mid-February, as well as the downturn in March, can be attributed to the decrease in activity by the Xor.DDoS bot family, which made a significant contribution to the statistics.



Number of DDoS attacks over time* in Q1 2017

** DDoS attacks may last for several days. In this timeline, the same attack may be counted several times, i.e. one time for each day of its duration.*

The distribution of DDoS activity by day of the week saw little change from the previous quarter. Saturday was the busiest day of the week in Q1 for DDoS attacks (16.05% of attacks). Monday remained the quietest day of the week (12.28%).

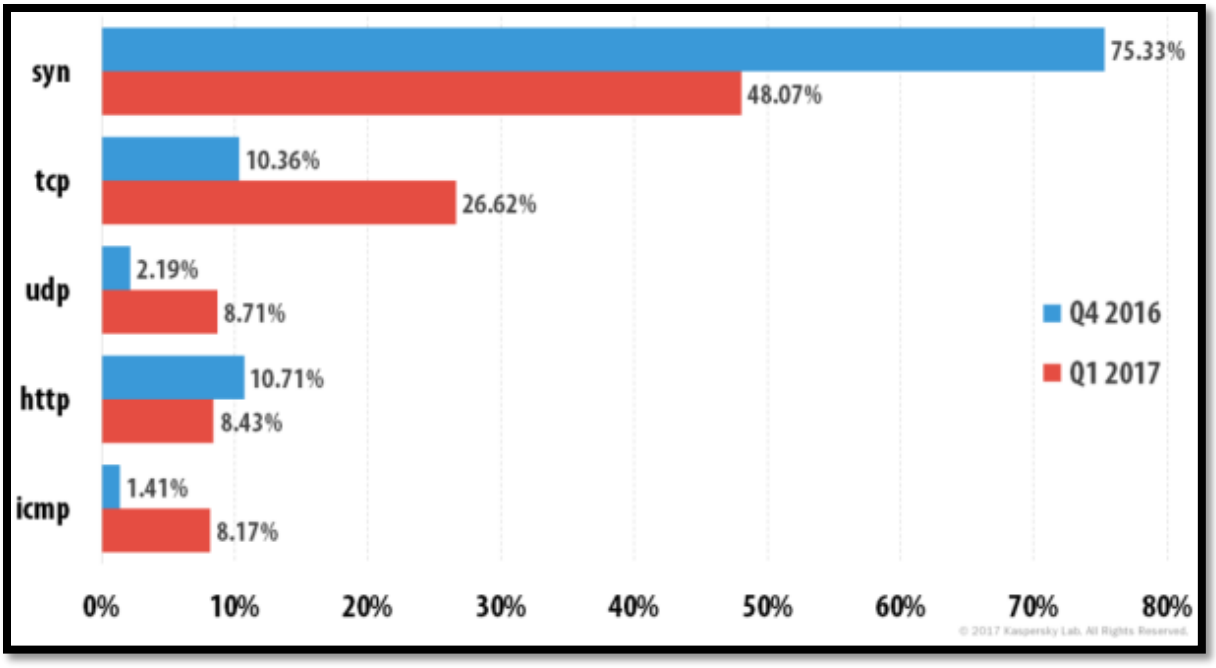


Distribution of DDoS attack numbers by day of the week, Q4 2016 and Q1 2017

Types and duration of DDoS attacks

In the first quarter of 2017, there was a sharp increase in the number and proportion of TCP DDoS attacks – from 10.36% to 26.62%. The percentage of UDP and ICMP attacks also grew significantly – from 2.19% to 8.71% and from 1.41% to 8.17% respectively. Meanwhile, the quarter saw a considerable decline in the share of SYN DDoS (48.07% vs. 75.33%) and HTTP (from 10.71% to 8.43%) attacks.

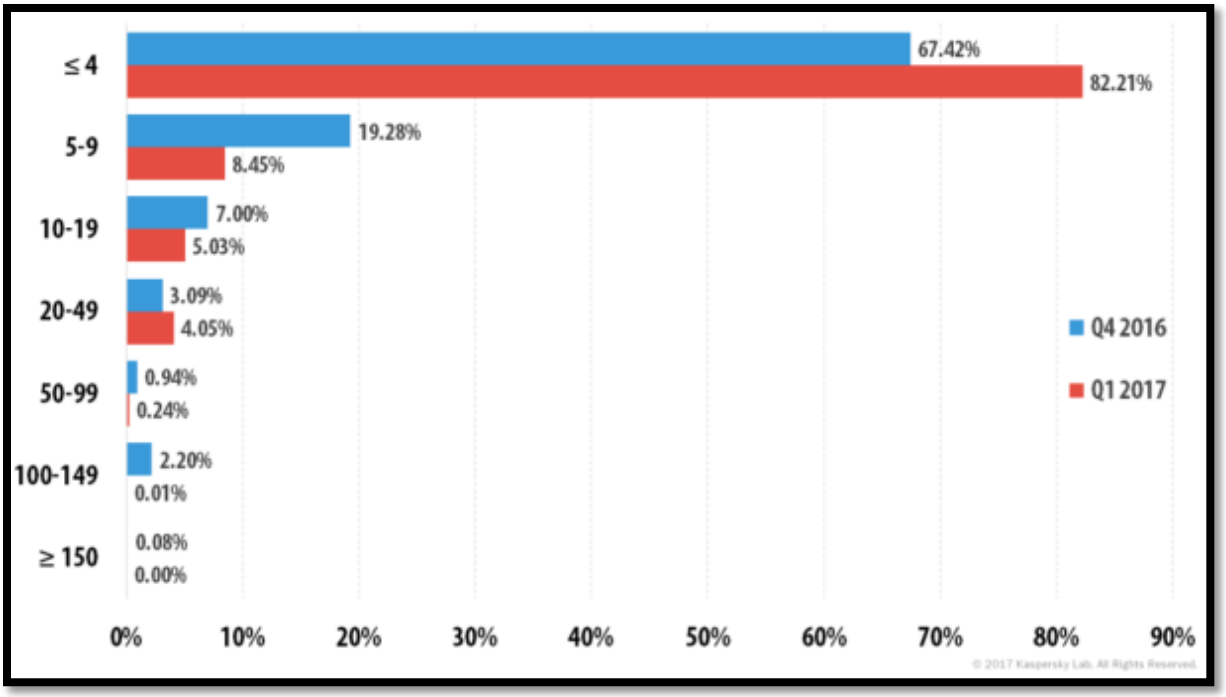
The increase in the proportion of TCP attacks was due to greater bot activity by the Yoyo, Drive and Nitol families. The growth in ICMP attacks is the result Yoyo and Darkrai activity. Darkrai bots also began conducting more UDP attacks, which was reflected in the statistics.



Distribution of DDoS attacks by type, Q4 2016 and Q1 2017

In the first quarter of 2017, few attacks lasted more than 100 hours. The biggest proportion of attacks lasted no more than four hours – 82.21%, which was 14.79 p.p. more than in the previous quarter. The percentage of even longer attacks decreased considerably: the share of attacks lasting 50-99 hours accounted for 0.24% (vs. 0.94% in Q4 2016); the share of attacks that lasted 5-9 hours decreased from 19.28% to 8.45%; attacks lasting 10-19 hours fell from 7% to 5.05%. Meanwhile, the proportion of attacks that lasted 20-49 hours grew slightly – by 1 p.p.

The longest DDoS attack in the first quarter lasted for only 120 hours, 172 hours shorter than the previous quarter's maximum.

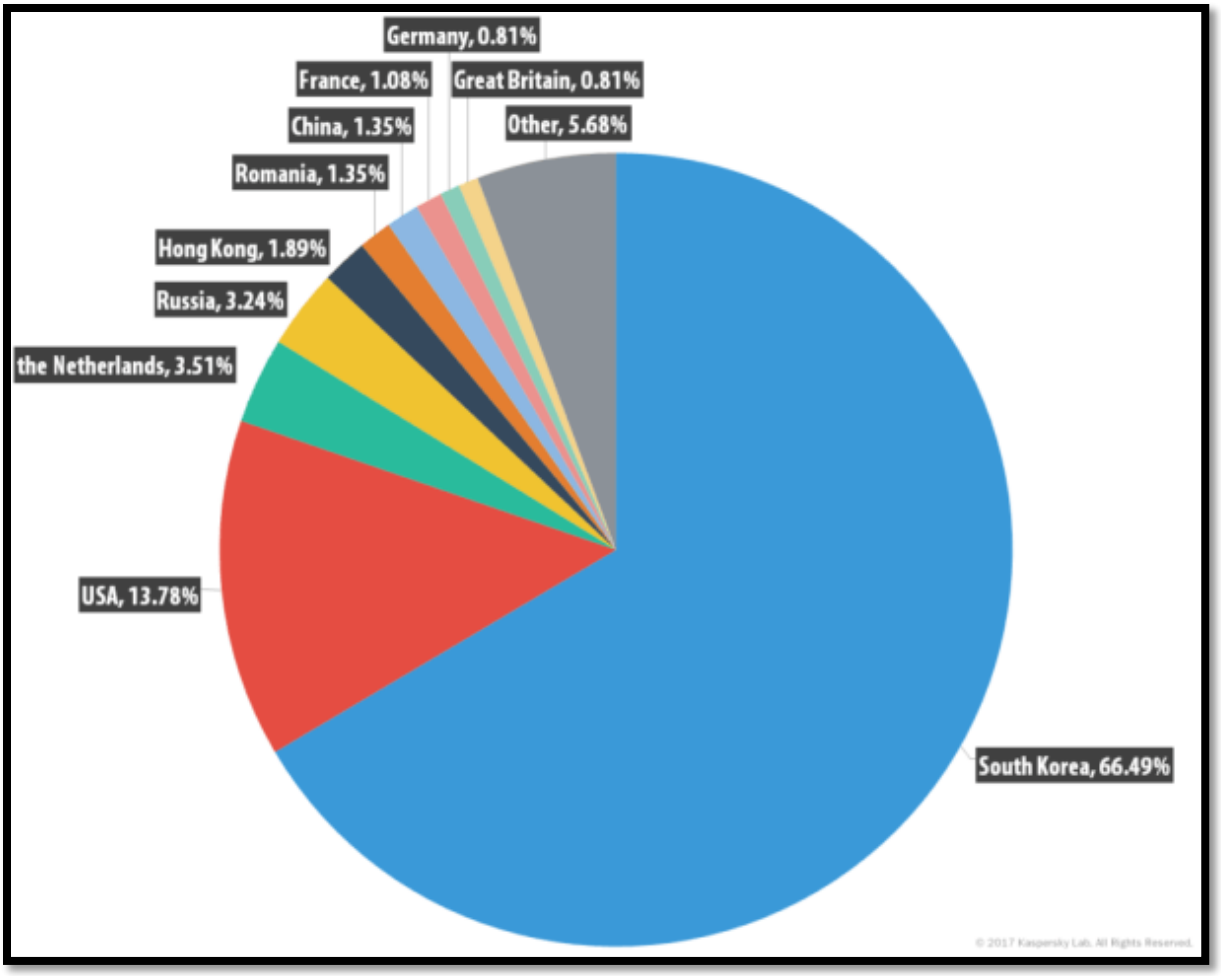


Distribution of DDoS attacks by duration (hours), Q4 2016 and Q1 2017

C&C servers and botnet types

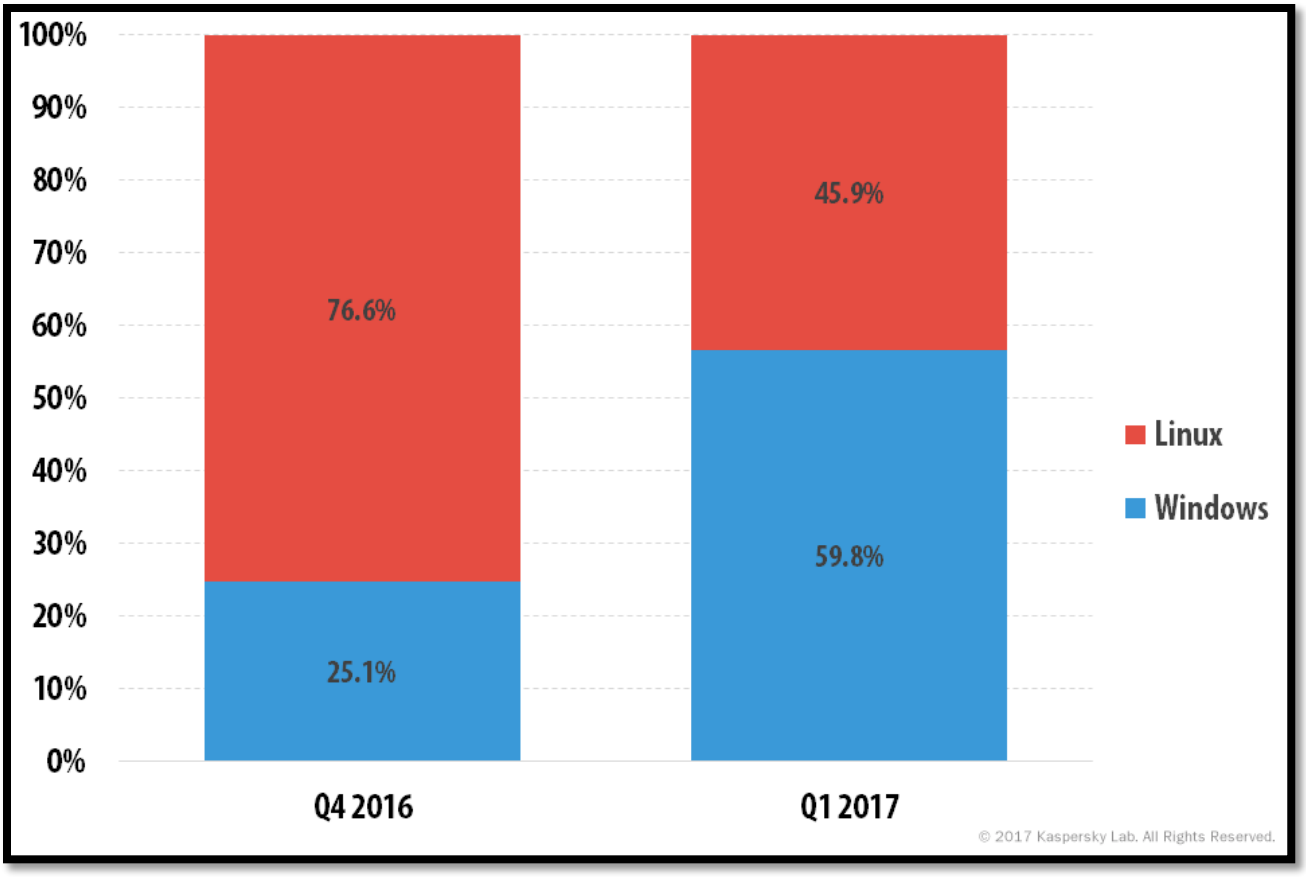
In Q1, the highest number of C&C servers was detected in South Korea: the country's contribution increased from 59.06% in the previous quarter to 66.49%. The US (13.78%) came second, followed by the Netherlands with 3.51%, which replaced China (1.35%) in the Top 3 countries hosting the most C&C servers. The total share of the three leaders accounted for 83.8% of all detected C&C servers.

The Top 10 also saw considerable changes. Japan, Ukraine and Bulgaria left the ranking and were replaced by Hong Kong (1.89%), Romania (1.35%) and Germany (0.81%). Of special note was China's sharp decline: the country dropped from second place to seventh.



Distribution of botnet C&C servers by country in Q1 2017

The distribution of operating systems changed drastically in Q1: Windows-based DDoS bots surpassed the trendy new IoT bots, accounting for 59.81% of all attacks. This is the result of growing activity by bots belonging to the Yoyo, Drive and Nitol families, all of which were developed for Windows.



Correlation between attacks launched from Windows and Linux botnets, Q4 2016 and Q1 2017

The majority of attacks – 99.6% – were carried out by bots belonging to a single family. Cybercriminals launched attacks using bots from two different families in just 0.4% of cases. Attacks involving bots from three families were negligible.

Conclusion

Although the first quarter of 2017 was rather quiet compared to the previous reporting period, there were a few interesting developments. Despite the growing popularity of IoT botnets, Windows-based bots accounted for 59.81% of all attacks. Meanwhile, complex attacks that can only be repelled with sophisticated protection mechanisms are becoming more frequent.

In Q1 2017, not a single amplification attack was recorded, which suggests that their effectiveness has declined. We can assume that this type of attack is gradually becoming a thing of the past. Another trend evident this quarter is the rise in the number of encryption-based attacks. However, it cannot be described as significant yet.