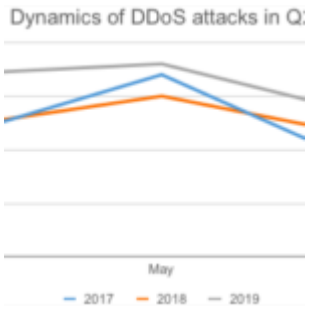
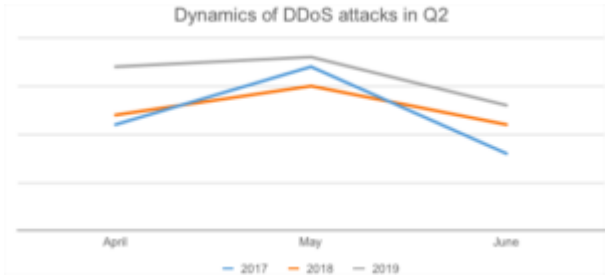
Summertime and the DDoS is easy: Q2 saw 18% rise in attacks compared to last year





In the second quarter of 2019, the total number of DDoS attacks grew by 18%, compared to the same period in 2018. Application-layer attacks, which are more difficult to organize and protect against, showed significant growth – increasing in quantity by a third (32%) compared with Q2 2018. As a result, they now constitute almost half (46%) of all attacks prevented by Kaspersky DDoS Protection.

According to Kaspersky's DDoS Q2 2019 report, the number of attacks in the second quarter of 2019 is
44% less than in Q1, which is not unexpected as such attacks usually reduce in activity in late spring and summer. However, compared with the same period last year, the quantity of DDoS attacks in Q2 increased by 18% and by 25% when compared with Q2 2017.

April MayJune

Dynamics of DDoS attacks in Q2

201720182019

Notably, the seasonal decrease only had a negligible effect on the number of attacks on the application
layer, reducing by just 4% compared to the previous quarter. These type of attacks target certain functions or APIs of applications in order to consume not only the network, but server resources as well.

They are also harder to detect and protect from, as they include the performing of legitimate requests.

When compared with Q2 2018, the quantity of these type of attacks has increased by nearly a third (32%) and the share of such attacks in Q2 2019 rose to 46%. This is a nine percent increase in share than the first quarter of the year, and 15% more in the same period of 2018.

"Traditionally, troublemakers who conduct DDoS attacks for fun go on holiday during the summer and

give up their activity until September. However, the statistics for this quarter show that professional attackers, who perform complex DDoS attacks, are working hard even over the summer months. This
trend is rather worrying for businesses. Many are well protected against high volumes of junk traffic, but
DDoS attacks on the application layer require to identify illegitimate activity even if its volume is low. We
therefore recommend that businesses ensure their DDoS protection solutions are ready to withstand these complex attacks," comments Alexey Kiselev, Business Development Manager on the Kaspersky DDoS Protection team.

Summertime and the DDoS is easy: Q2 saw 18% rise in attacks compared to last year
The analysis of commands received by bots from command and control (C&C) servers revealed that the
longest DDoS attack of Q2 2019 lasted 509 hours – almost 21 days. This is the lengthiest attack since
Kaspersky started to monitor botnet activity in 2015. Previously, the longest attack lasted 329 hours and
was registered in Q4 2018.
To help organizations protect themselves from DDoS attacks, Kaspersky recommends taking the following steps:
 Ensure that web and IT resources can handle high traffic
 Use professional solutions to protect the organization against attacks. For example, Kaspersky DDoS Protection combines Kaspersky's extensive expertise in combating cyberthreats and the company's unique in-house developments. The solution protects against all types of DDoS attacks regardless of their complexity, strength or duration
Read the full text of the report on Securelist.
About Kaspersky
Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and
security expertise is constantly transforming into innovative security solutions and services to protect
businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users
are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters
most to them. Learn more at www.kaspersky.com.