IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

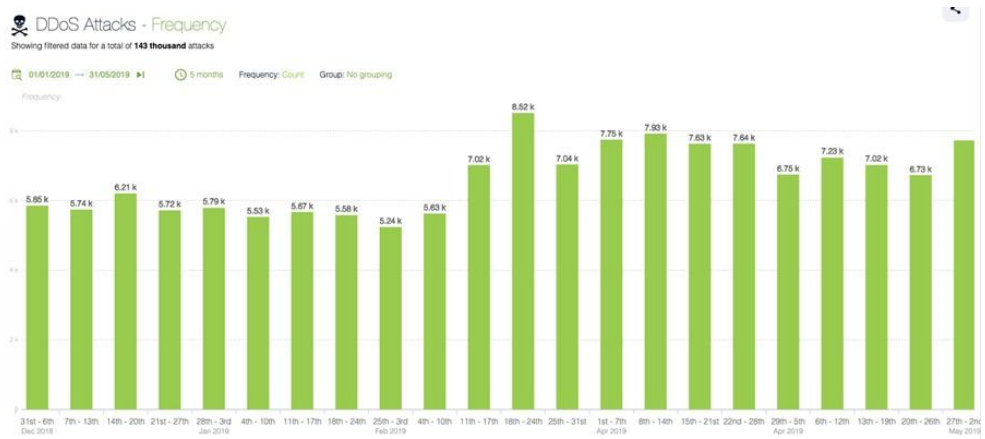
DDos Attacks – UK in Focus

NETSCOUT Arbor

Analysis

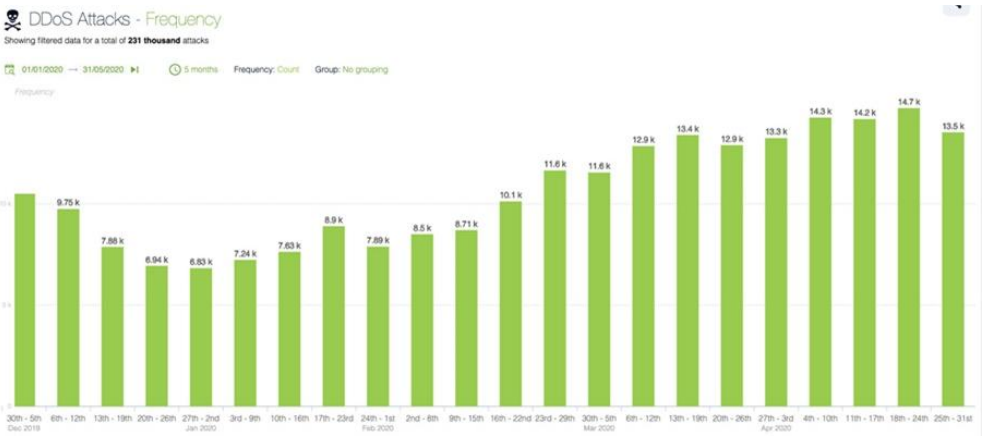
Our Advanced Threat Level Analysis System (ATLAS), which processes DDoS information from more than 300 large ISP networks worldwide, recorded more than 248,000 attacks against entities in the United Kingdom in 2020 from 1 January to 31 May (*see Figure 2*). This is a 62% increase when compared with the same period in 2019, when we observed 143,000 attacks (*see Figure 1*).

Figure 1: DDos attacks – frequency



Through the end of January 2020, we observed a constant growth in the overall DDoS attack rate as organizations continue to experience heightened levels of malicious traffic (*see Figure 2*).

Figure 2: DDos attacks – frequency



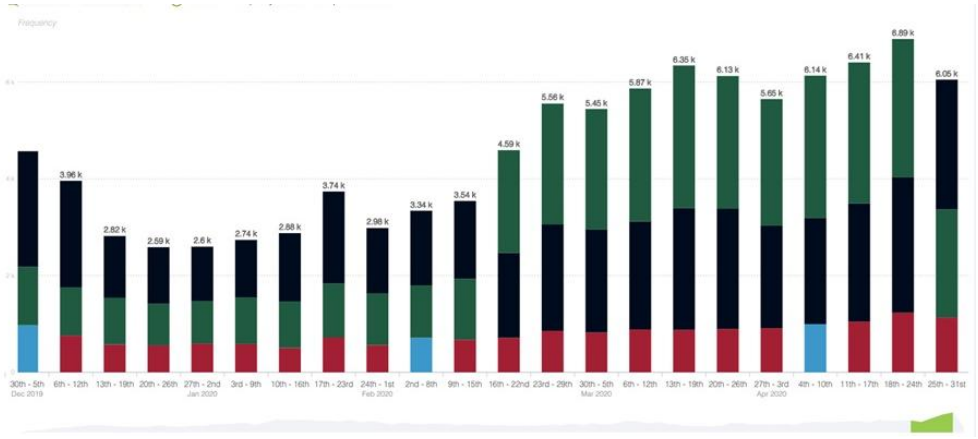
IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Most common DDoS attack vectors

Looking at specific DDoS attack vectors, we can see that the majority of observed attacks during this period were volumetric in nature. These attacks typically rely on relatively high rates of packets-per-second (pps) and/or bits-per-second (bps) in order to overwhelm targeted servers, services, applications, and network capacities. Observed targets ranged from individual IP addresses to larger network blocks via 'carpet-bombing' attack addressing techniques. For DDoS attacks in the United Kingdom during the period in question, DNS reflection/amplification were the most common; this is unsurprising, given the relatively large number of abusable open DNS recursors present on the Internet today.

Figure 3: DDos attacks – frequency



Note: The graph shows only the most common individual vectors. Multi-vector attacks and uncommon vectors are elided.

In addition to DNS reflection/amplification attacks, we also observed approximately 20 different UDP-based DDoS attack vectors; CLDAP reflection/amplification attacks were the most prominent among them. The relative breakdown of commonly-observed DDoS attack vectors during this period in the UK was in line with trends globally.

Average attack bandwidth

In this graph, we can see that the average attack bandwidth in the UK so far this year has been right around 1gb/sec. While a single 1gb/sec attack may not sound significant in a world where attacks in the hundreds of gb/sec are commonplace, the reality is that most DDoS attacks are far larger than what is necessary to overwhelm their targets, and so these 'smaller' attacks are in fact operationally significant.

Further, looking at the aggregate numbers for observed DDoS attack bandwidth in total, the start of 2020 saw a significant 56% increase to 260.59tb/sec (*see Figure 4*), as opposed to the 166.77tb/sec observed during the same interval in 2019 (*see Figure 5*).

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Figure 4: DDos attacks – frequency

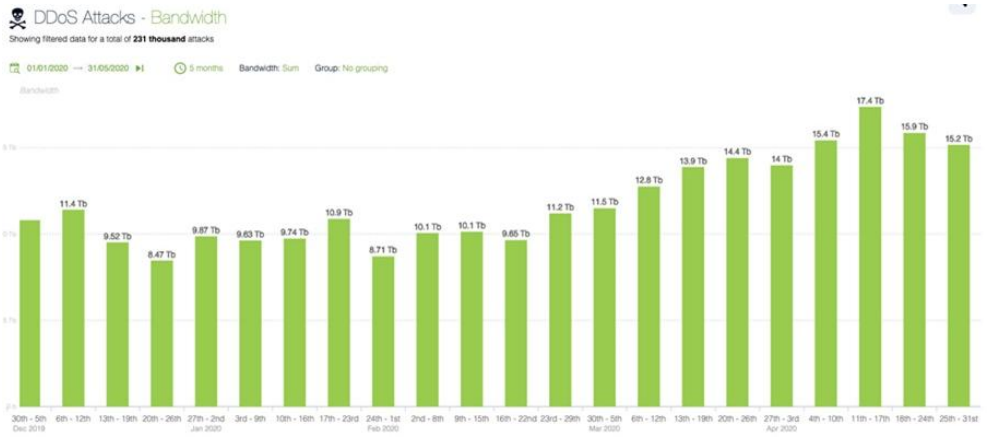
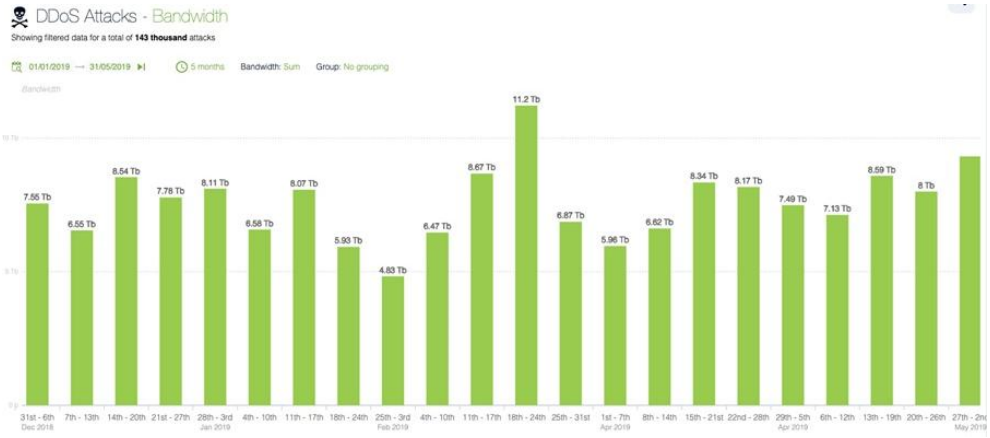


Figure 5: DDos attacks – frequency



Maximum observed attack bandwidth

So far, the largest single DDoS attack we've observed in the UK this year is a 488gb/sec attack targeting an organization in the Telecommunications vertical. To put this into perspective, the largest DDoS attack we've observed to date worldwide is 1.7tb/sec; the largest attack we observed in the UK in all of 2019 was 352gb/sec, so this represents a 39% increase for the largest observed DDoS attack in the UK, year-over-year.

DDoS attack throughput

Another important we track is the throughput, or packets per second (pps) for DDoS attacks. Just as with the frequency and bandwidth noted above, the throughput for attacks destined for the United Kingdom also saw 47% increase in the aggregate total of pps from January 1st to May 31st (*see Figure 6*) as compared to the same time period in 2019 (*see Figure 7*).

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Figure 6: DDos attacks – frequency

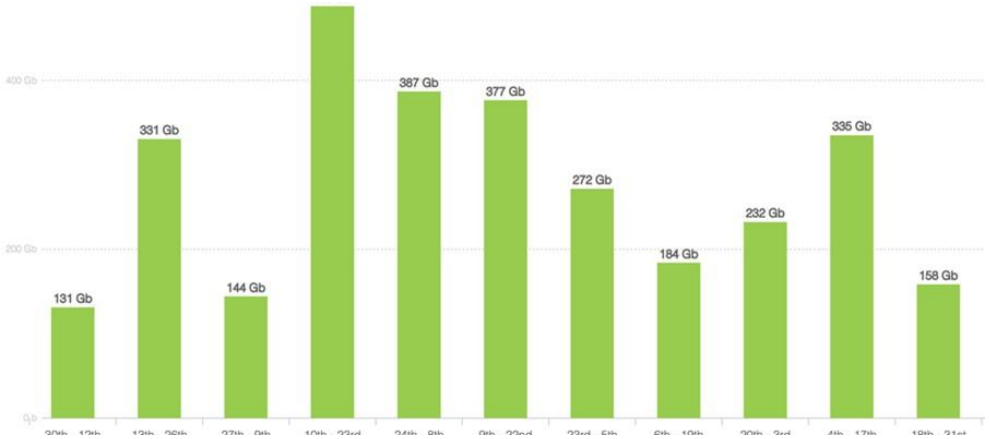


Figure 7: DDos attacks – frequency

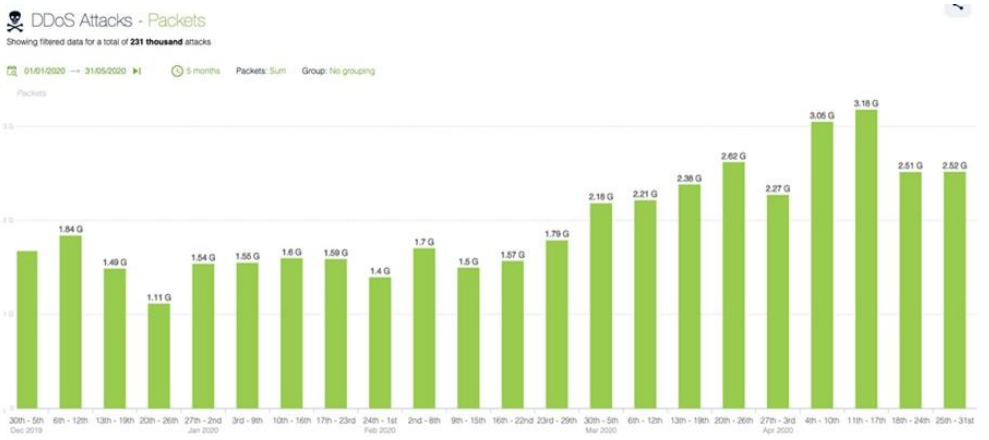
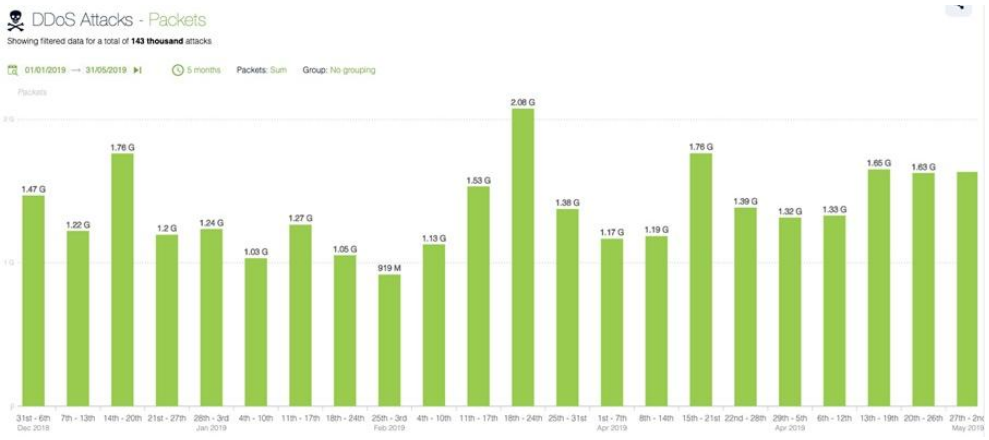


Figure 8: DDos attacks – frequency



IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Conclusion

We are not yet halfway through 2020, and it is quite likely that the size and impact of DDoS attacks will continue to grow in scale. Comparing all of these charts side by side, it is apparently that the overall trend in attack volumes is increasing, and we anticipate that will continue through the rest of the year.

Given that the largest observed attack this year to date preceded the full onset of the ongoing COVID-19 pandemic – and all the changes in online usage and behaviours that this has brought about – it is a reminder that organisations are exposed to an underlying, perpetual risk of a significant impact of DDoS attacks on their online presences and properties.

In addition to the analysis NETSCOUT uses for these metrics, we also make a visual representation of these attacks available to view and analyse on https://www.netscout.com/horizon