UNIVERSITY OF CAMBRIDGE

**Cambridge Cybercrime Centre**
**COVID Briefing Paper # 7**

# DoS Attacks During Lockdown: Worldwide Data

**Ruba Abu-Salma**

**August 18, 2020**

## Executive summary

Cambridge Cybercrime Centre (CCC) COVID Briefing Papers are an ongoing series of short-form, open-access reports aimed at academics, policymakers, and practitioners, which aim to provide an accessible summary of our ongoing research into the effects which the coronavirus pandemic (and government responses) are having on cybercrime.

In this report, we build on the findings of Briefing Paper #6 which examined data on denial-of-service (DoS) attacks in Europe. Here, we look at the worldwide picture, finding that attacks grew during lockdown in the US, Brazil, and China. As with the European data, we see that peaks occur in school holidays.

## Reflective UDP amplification DoS attacks worldwide

In Briefing Paper #3, we examined the dramatic rise in attacks bought from DoS-for-hire websites during lockdown. In Briefing Paper #6, we looked at European-country level data, finding some increase during lockdown but the main spike occurring at the start of the Easter holidays.

In this report, we look at worldwide totals for reflected UDP amplification DoS attacks as measured by our sensor network (Briefing Paper #6 gives all the details). As can be seen in Figure 1, these totals are dominated by attacks on Brazilian, Chinese, and, overwhelmingly, US IP addresses.

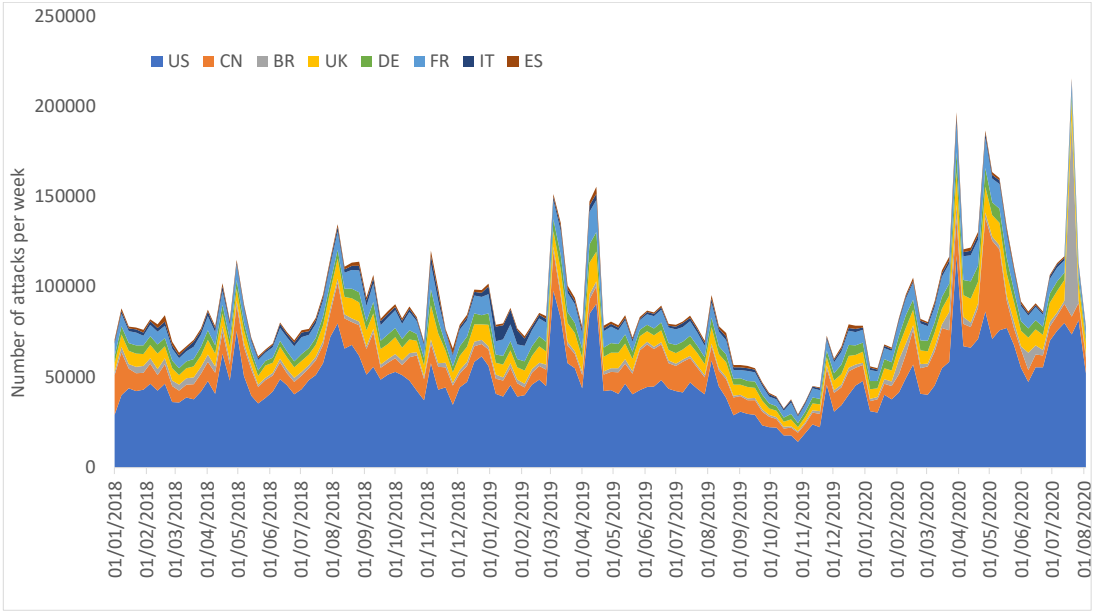


Figure 1: A stacked area graph showing total DoS attack numbers per week split by country of victim (January 1, 2018 – August 1, 2020).

As coronavirus cases started to increase, China imposed 'localized' lockdowns on January 26th, 2020. The US and Brazil went into localized lockdown on March 17th.[1] As shown in Figure 2, there has been

a general increase in DoS attacks during the first two quarters of 2020 in Brazil (plotted in gray), China (plotted in orange), and the US (plotted in dark blue). Although lockdown has clearly had an impact on numbers, there must be other factors involved, because the rise in attacks on Chinese IP addresses does not start seven weeks earlier than elsewhere.

Attacks on US IP addresses peak at 117 373 in the week of March 30th (a week before the Easter holiday). The attacks on Brazilian IP addresses also peak during the same week.[2] The peak of 54 582 attacks on Chinese IP addresses occurs a week later.

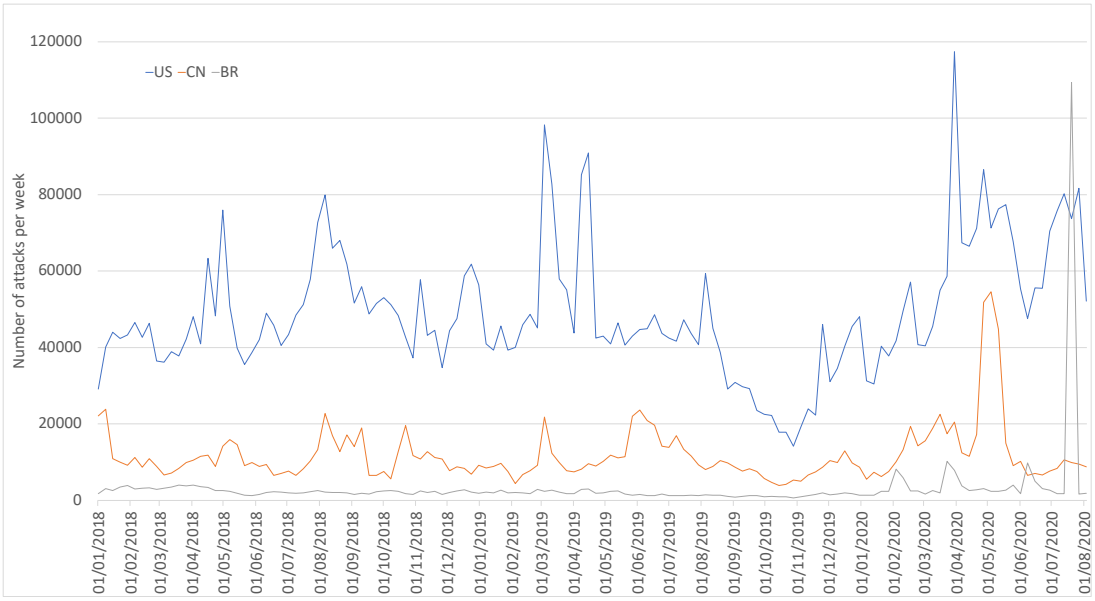


Figure 2: Total DoS attacks per week in Brazil, China, and the US (January 1, 2018 – August 1, 2020).

## Conclusions

There has been a rise in attacks in the US and Brazil, which we attribute to the lockdown as well as school holidays (viz. Easter). We see a similar pattern of attacks in China, although less directly linked to lockdown. China also cancelled Lunar New Year festivities in 2020,[3] to prevent families from gathering. As a result, we speculate, children and young people spent much of their time at home playing online games – and it seems that a minority chose to cheat by purchasing DoS attacks.

[1] Coronavirus: The world in lockdown in maps and charts: `https://www.bbc.co.uk/news/world-52103747`.
[2] The highest total for Brazil is 109 315 on July 20th, but this is only a one-week event.
[3] Lunar New Year, or Spring Festival, is the most important celebration in the Chinese calendar. Canceling celebrations was a massive deal: `https://edition.cnn.com/2020/01/24/china/virus-lunar-new-year-intl-hnk-scli/index.html`.



The full set of CCC COVID Briefing Papers can be found at: `https://cambridgecybercrime.uk/COVID`