UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 6

Denial of Service Attacks during Lockdown: the role of Easter

Richard Clayton

11 August 2020

Executive summary

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 take a further look at some of the data we hold about Denial of Service (DoS) attacks. In COVID Briefing Paper #3 we showed that the purchase of DoS-for-hire had risen substantially during lockdown. Here we examine data from our sensor network which records the identity of victims of 'reflected amplified UDP attacks'.

We hypothesised that we might be able to show that there was a marked increase in attacks during lockdown periods – and by breaking out data for individual countries, which entered lockdown at different times, we might show that the rise occurred at different times. We did not find this effect – in fact the data we have for the UK, Spain and Italy shows a general rise in attacks from the turn of the year all the way to Easter – and then a decrease since then. A year earlier, attacks didn't generally grow so much during the winter months, but the same spike occurs at Easter.

Denial of service using reflected amplified UDP

In a reflected amplified UDP attack small amounts of traffic is sent to misconfigured machines which reply with far more data. By forging the source of the request an attacker can ensure that a victim receives very significant streams of traffic, overwhelming their connection. We've been running sensors that pretend to be these misconfigured machines, and thereby collecting data on the victims of these attacks, since 2014 [1].

The consensus is that the majority of DOS-for-hire attacks are bought by people who wish to cheat at online games by disrupting opponents (or they just wish to show their displeasure at losing), and many of the attacks that they purchase use reflected amplified UDP.

Many online games group players by location – for reasons of performance, language or indeed just because people wish to play people they know. Hence – and yes, we know this is just sketching out a multi-step argument, but see published papers such as [2] for more details – if we see a victim on a Spanish IP address it is reasonable to assume that the attacker is Spanish as well, victims in Italy are being attacked by Italians and so on.

Italy went into lockdown on the 9th of March, Spain on the 15th and the UK on the 23rd and we already know that DOS-for-hire attacks went up considerably during lockdown. Therefore, we might expect to see increases in attacks on Italian IP addresses some two weeks earlier than attacks on UK IP addresses.

Figure 1 shows what we actually observed – attacks on UK addresses are plotted in red and peak at 18080 attacks in the week of 30th March, the start of the Easter holidays (Easter Sunday was 12th March). Attacks on Italian IP addresses are plotted in blue and peak at 3008 the same week (the graph has been scaled for clarity, use the right hand Y-axis). Attacks on Spanish IP addresses peak at 2458 exactly the same week (the same scaling has been applied to these).

Perhaps not surprisingly, the previous peak was at Christmas, but although there is some drop-off in January, there is some growth through February and March.

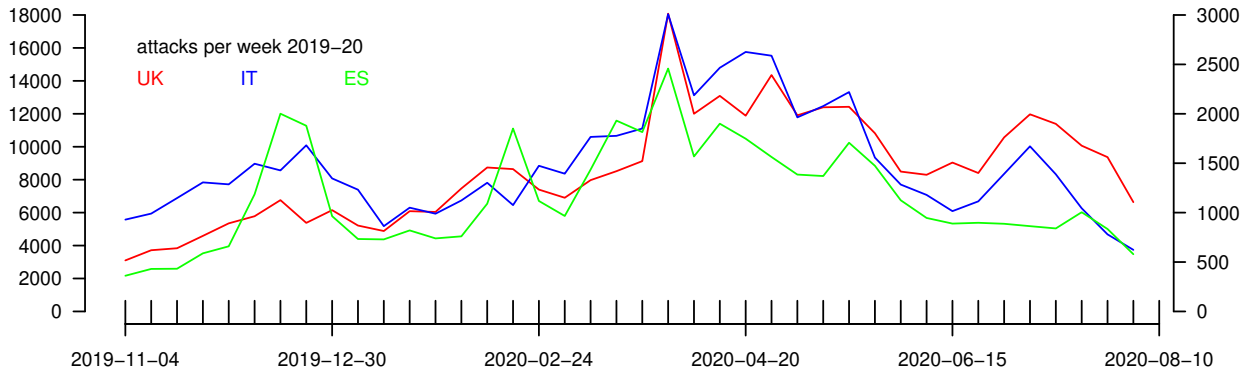

Figure 1: Reflected amplified DoS attacks per week, from November 2018, for victim addresses in the UK (red line, left-hand scale), Italy (blue line, right-hand scale) and Spain (green line, right-hand scale).

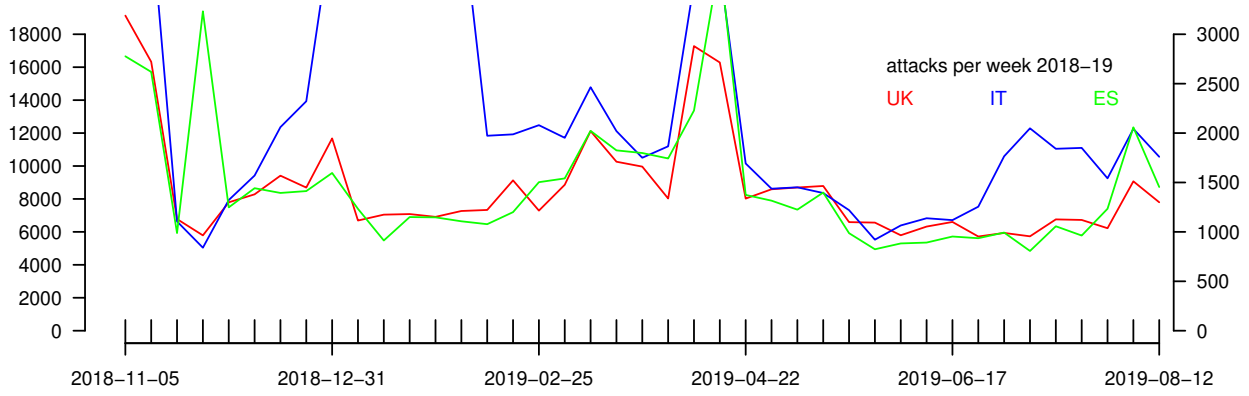

Figure 2: Reflected amplified DoS attacks per week, from November 2019, for victim addresses in the UK (red line, left-hand scale), Italy (blue line, right-hand scale) and Spain (green line, right-hand scale).

If we compare this with the previous year then we again see peaks at Christmas and just before Easter (Easter Sunday 2019 was 21st April) . . . but there's a lot more activity in Italy (which hit 8000 or more attacks a week for all of January 2019). However, for Spain and the UK the figures show rather less of an increase during the rest of the winter,

Conclusions

Our data shows that, in the UK, Italy and Spain, there was far more reflected amplified UDP DoS activity during the Easter holidays 2020 than in 'term time' – despite the lockdown. There is evidence for a small amount of growth during February and March, but nothing like the huge increases we've previously reported upon for worldwide data.

[1] D. R. Thomas, R. Clayton and A. R. Beresford (2017). 1000 days of UDP amplification DDoS attacks. 2017 APWG Symposium on Electronic Crime Research (eCrime).
[2] B. Collier, D. R. Thomas, R. Clayton and A. Hutchings (2019). Booting the booters: Evaluating the effects of police interventions in the market for Denial-of-Service attacks. Internet Measurement Conference (IMC '19)

At the Cambridge Cybercrime Centre we make our research data available to other academics, sometimes before we have looked at it ourselves! Researchers can be provided access to our 'CrimeBB' dataset of (26 and counting) underground cybercrime forums, our extensive collections of chat channel data, and our new collections of forums relating to online right-wing extremism and radicalisation. We can also share email spam and sensor data related to DDoS and IoT malware. All these collections are regularly updated and can be rapidly provided under license – for full details see: `https://cambridgecybercrime.uk`