UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 3

The Impact of Lockdown on DoS-for-hire

Richard Clayton

21 July 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.

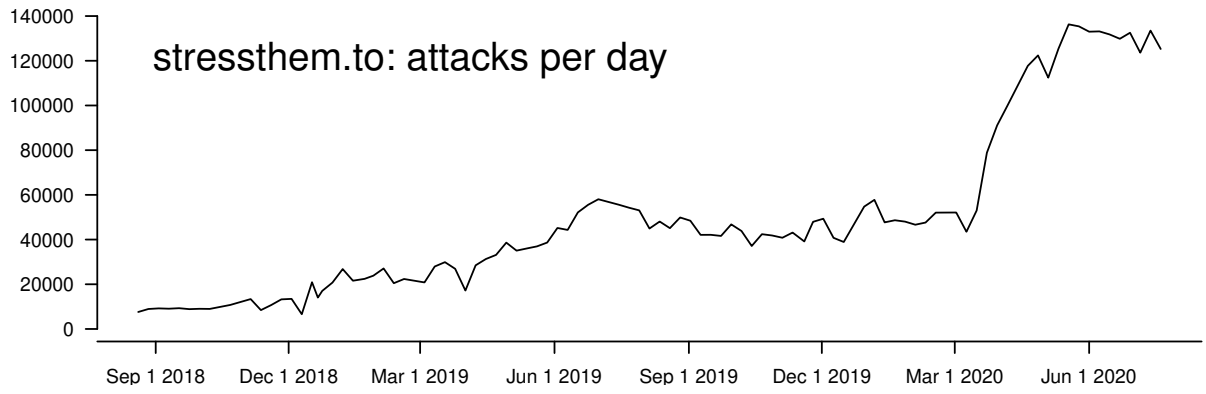
In this report, we look at the impact of lockdown on Denial of Service (DoS) activity through the lens of the self-reported usage of the most active DoS-for-hire service. We find a substantial rise in the figures from early March to mid May, almost certainly caused by cheating within online games. The number of attacks has trebled and the number of new website users has grown more than fivefold. However, there is increased activity across the board and so this website has only increased its market share by a few percentage points.

Booter websites

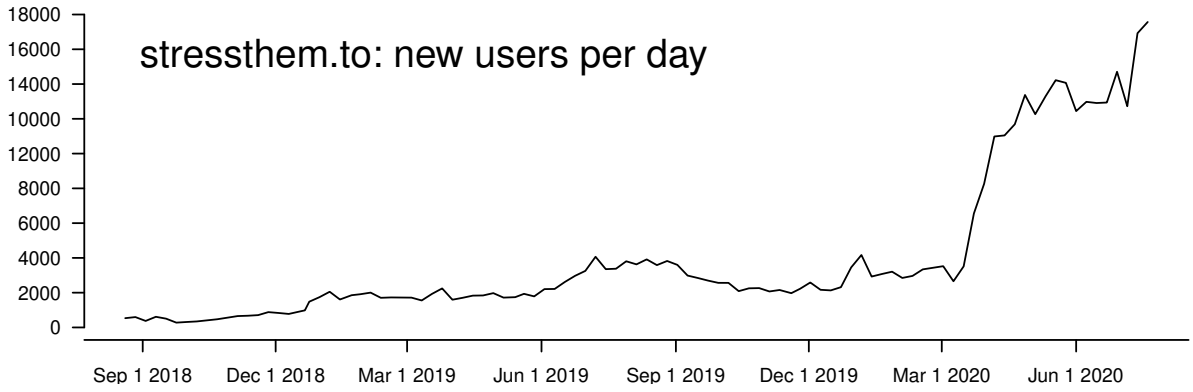
Denial of service (DoS) attacks involve overloading a website or computer system with so much bogus traffic that legitimate access fails. The websites selling DoS attacks for a fee are termed 'booter' or 'stresser' services. The term 'booter' comes from the malicious act of 'booting' a games player out of an online game, with 'stresser' being a common figleaf – that one is testing one's own servers to assess resilience.

There are around 50 booter websites active at any given time, though less than a dozen do substantial levels of business. Around three-quarters of the services market themselves by providing running totals of the number of attacks they sell – data that we believe to be generally reliable (see [1] for a detailed explanation of this) – and we have been regularly collecting this activity data for several years.

Looking at the total number of attacks per day of stressthem.to, which we currently believe to be the market leader, shows that steady growth through the first half of 2019 was followed by fairly stable levels of activity. But the numbers of attacks took off from early March until mid-May, before settling down again to around 130 000 attacks per day (most of a million attacks a week).

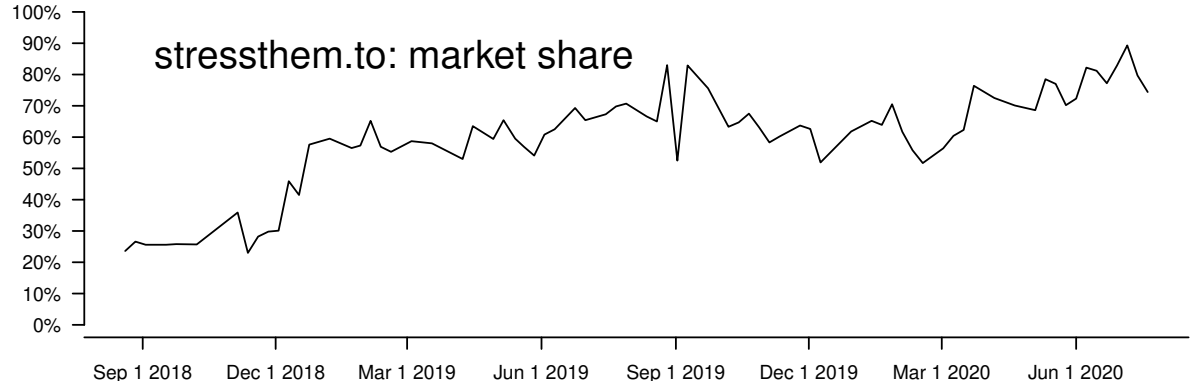


The stressthem.to website also reports the number of users who have registered for an account and this shows similar increases in activity (not surprisingly since most users only purchase a few attacks right at the start of their membership). Of these new users only a proportion (perhaps only 1 in 20) will actually purchase any attacks, but with 16 000 new users per day and plans starting at just $9.99 for a couple of days of service, turnover for this website may now be in the two to three million dollars a year range.



Another interesting way of looking at this data is to consider what the market share might be. Since a number of booters do not report any statistics this will be an overestimate (by perhaps 10% or so), but it can be seen that from being about a quarter of all attacks in September 2018 stressthem.to's market share rose quickly in early 2019. This is almost certainly a direct result of the FBI seizing 15 booter domain names just before Christmas 2018 (thereby shuttering eight booters) – stressthem.to was not targeted in that operation.

As can be seen, in the period since March the market share has increased slightly but there is not the dramatic rise of the other graphs. This tells us that other booters are also doing more attacks in this period.



Conclusions

Lockdown has resulted in a lot of people being stuck at home with time on their hands, and a lot of them have been playing computer games (the large games companies are reporting record sales and record levels of engagement). A small number of those gamers have been cheating by attempting to boot their opponents off the game, or slow them down so as to get an advantage. This has led to dramatic rises in the number of attacks bought from DoS-for-hire websites – and we've charted the increase at the biggest such website.

It's likely that there are other Denial of Service targets too – DoSing a school website serving up your Maths homework may be attractive to some, as is DoS for extortion purposes and DoS for political reasons (US police websites, for example). In a future briefing we'll be looking at what the targets might actually be. In the meantime it's worth remembering that being 'the biggest' is generally a career-limiting move for cybercrime infrastructure and so in due course we would expect these charts to drop to zero.

[1] B.Collier, D.R.Thomas, R.Clayton and A.Hutchings: Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks. In: Proceedings of the Internet Measurement Conference (IMC), 2019.

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`

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