UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 15

Measuring Malware Hosting 'Whack-a-Mole'

Richard Clayton

13 October 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.

Here we look at our data on the hosting of malware which targets 'Internet of Things' (IoT) devices. Our honeypots detect this malware and record where it is hosted. We, along with other organisations collecting similar datasets, share this data with the security community. This should lead to 'take-down' of the illegal malware-serving sites, which, of course, are immediately replaced by their operators. In this paper, we analyse some of the ebbs and flows of this 'whack-a-mole' game.

Counting the sites that serve malware

IoT malware is spread by the guessing of weak passwords on IoT devices and the exploitation of unpatched software vulnerabilities. Our honeypots *pretend* to be vulnerable, allowing them to become targets, to capture any new malware samples when they are attacked, and to identify the malware's 'back-end' hosting server. The total number of servers which we can detect that are hosting this malware per day is plotted in Figure 1. As can be seen the number of servers ebbs and flows over time, being influenced partly by how many malware operators are active and partly by how many servers they choose to operate in parallel. This itself depends, of course, on their view as to how long they are likely to operate before being 'taken down'.

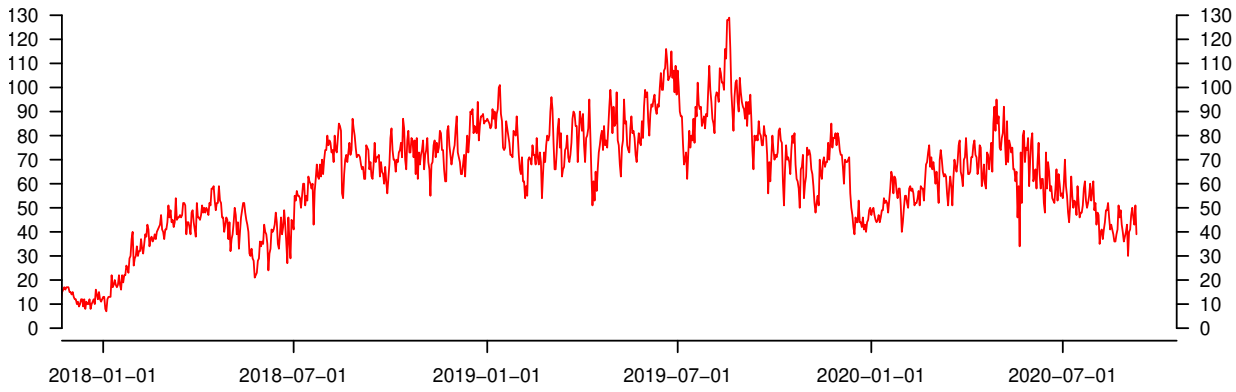

Figure 1: Number of distinct IPs serving IoT malware: January 2018 to mid September 2020

Figure 2 shows the data for the US company hosting the largest number of servers over time – this sometimes accounts for over half the active servers. Also plotted is the average lifetime of the servers operating on each day (measured in hours). This gives an insight into the hosting company's efforts to deal with malware servers; rapid drops in average lifetime indicate a blitz on long-lived servers, whereas a fairly steady average lifetime indicates a steady state in which servers are removed about as fast as new ones are stood up. The overall jagged nature of the graphs indicates that there little anti-abuse activity at weekends. Since the pandemic started, overall numbers of malware servers has been lower, but they have stayed up considerably longer, which may reflect home-working difficulties for both 'attackers' and 'defenders'.

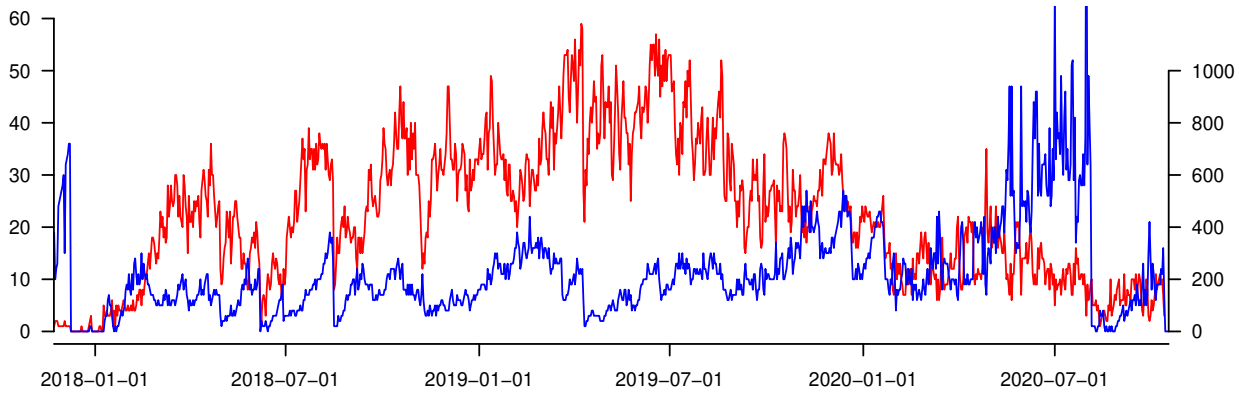

Figure 2: IoT malware servers at the most 'popular' hosting company: January 2018 to mid September 2020 (red: LH y-axis) along with their average lifetime in hours (blue: RH y-axis).

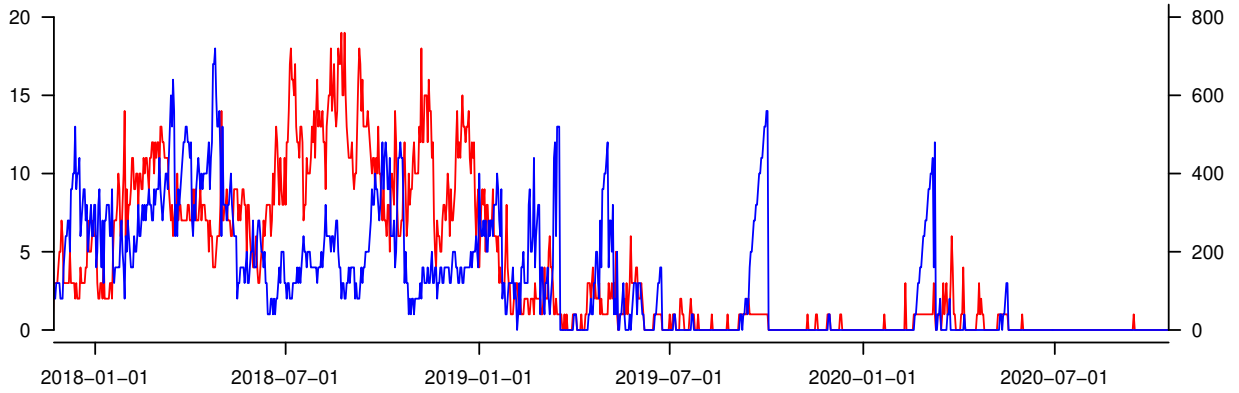

Figure 3: IoT malware servers at the second most 'popular' hosting company: January 2018 to mid September 2020 (red: LH y-axis) along with their average lifetime in hours (blue: RH y-axis).

Figure 3 shows the same type of graph for the second most 'popular' hosting company overall, based in Italy. Since early 2019 they have had only a handful of servers to deal with; however, the lifetime figures show that they can sometimes be pretty slow at doing so.

Conclusions

The data we have collected for the number and lifetimes of the servers of IoT malware show a situation in constant flux – the criminals are setting up new servers and the hosting companies are playing 'whack-a-mole' to get them removed. Close inspection of the graphs shows evidence of both steady state activity by the hosting companies and occasional 'blitzes'. This ongoing battle may seem like a waste of time for all concerned – but we have recently argued [1] that the boredom of constantly standing up new infrastructure is an important factor in causing those who operate this malware to reconsider their life choices.

[1] Ben Collier, Richard Clayton, Alice Hutchings and Daniel R. Thomas: *Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies*, Workshop on the Economics of Information Security (WEIS), 2020.

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 licence – for full details see: `https://cambridgecybercrime.uk`

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