UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 11

Analyzing DoS Attacks by UDP Protocol Used

Ruba Abu-Salma

September 15, 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 Briefing Paper #7, we examined worldwide totals for weekly reflected UDP amplification Denial-of-Service (DoS) attacks (as measured by our sensor network [2]). We found that these totals were overwhelmingly dominated by attacks on US and Chinese IP addresses. Here, we build on this by analyzing which UDP protocols are being used by attackers (focusing on the lockdown period). We find a steady increase in NTP attacks but considerable volatility in the number of LDAP and DNS attacks. The other UDP protocols we track are hardly used at all. Although our measurement of DNS is patchy, our LDAP figures are robust – so we think we are not only seeing changes in overall attacks but also some measurement bias caused by substantial changes by individual attackers.

Analyzing attacks by UDP protocol

We consider worldwide totals for reflected amplification DoS attacks, broken down by the UDP protocol used by attackers (see Figure 1). The overall rise in attack numbers from the beginning of 2020 appears to be largely driven by an increase in attacks using LDAP (plotted in yellow) along with NTP (plotted in dark blue). Other protocols are hardly used in comparison, except DNS (plotted in light blue).

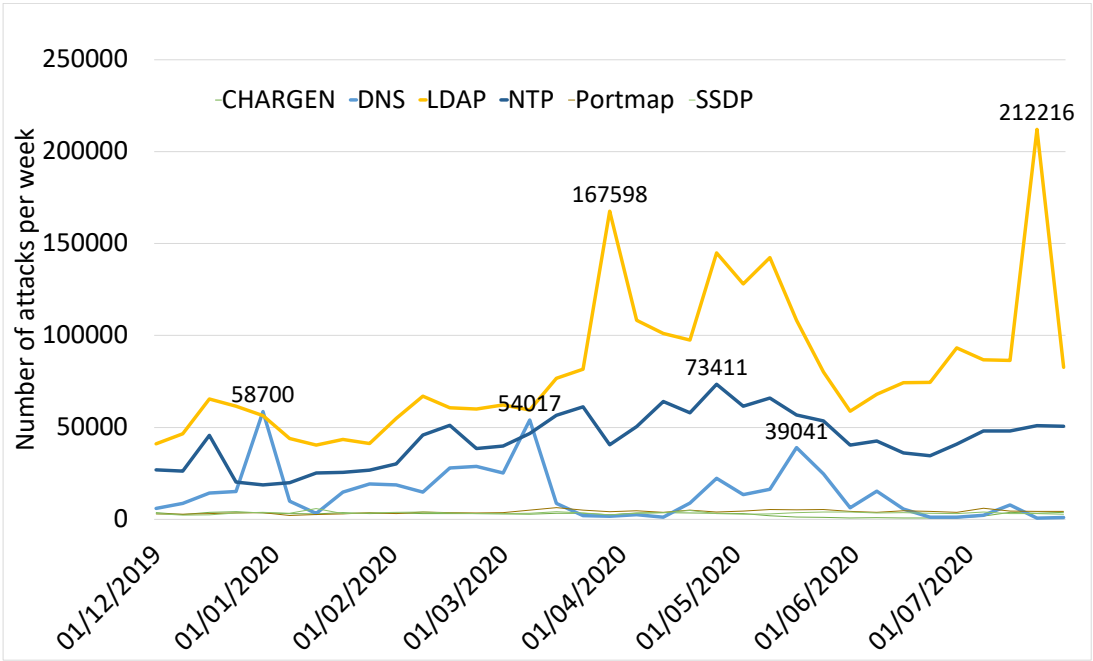

Figure 1: Total DoS attacks per week, split by UDP protocol used (Dec. 1, 2019 – Aug. 1, 2020).

LDAP-based DoS attacks have become popular because of LDAP's large amplification factor [1]. However, there are relatively few LDAP reflectors in the real world and, therefore, our sensors (honeypots) are often used in attacks, making our data representative of worldwide traffic [2]. Similarly, there are very few NTP reflectors, and, hence, we think our data is highly representative of total activity. However, for DNS the attackers have many millions of potential reflectors to choose from and, thus, our data collection is rather less complete, and our figures are rather less reliable.

To check our intuition, we used capture-recapture statistical analysis – using the Lincoln-Petersen estimator – to estimate the total number of DoS attacks worldwide, broken down by UDP protocol used. We also calculated error bars (representing standard deviation of uncertainty) for all the data points shown in Figure 1. The magnitude of these bars is small, with a median of 503, 444, and 338 weekly attacks for LDAP-, NTP-, and DNS-based attacks, respectively. Another way of viewing this is that the estimate of the coverage of attacks that we have is almost always well over 95% – so the variations are not attributable to the size of our sensor network but have other causes.

What, then, could cause the large variations in attack numbers we observe? Overall, as we have explained in earlier briefing papers, we attribute these changes to lockdown, and additionally to school holidays and closures. However, there are certainly other effects as well.

The changes may be because popular booters have added or removed attack types from the options that they offer their customers; alternatively, some minor changes in the description of the attacks may persuade those customers to select a particular style of attack. Also, booters do go offline from time to time – there have not been any significant law enforcement actions this year thus far, but hosting companies sometimes kick booters off their networks and disrupt service for a week or two. It is also possible that some of what we observe is merely booters 'refreshing' their lists of reflectors and, for whatever reason, adding or removing our sensors from the systems to which they will send traffic.

Conclusions

Although we have earlier presented a view of DoS attacks as having grown markedly during lockdown, with peaks attributable to the timing of school holidays, analysis of which UDP protocols are being used shows a more nuanced picture.

We find that there are only three UDP protocols in significant use in our data, and that the NTP data, which we believe is fairly accurate, broadly supports our earlier analysis. However, the DNS data, where our coverage is more patchy, is somewhat volatile. Nonetheless, there is evidence of a fairly rapid move away from DNS toward using LDAP. We also believe our LDAP data is fairly accurate overall, but some of the variation we measure may be caused by decisions by individual booter owners as to which reflectors to use, as well as reflecting overall trends in the market for DoS attacks.

References

[1] Fahmida Y. Rashid. "DDoS attacks abusing exposed LDAP servers on the rise". In: *InfoWorld* (2017). URL: `https://www.infoworld.com/article/3189756/ddos-attacks-abusing-exposed-ldap-servers-on-the-rise.html`.

[2] Daniel R. Thomas, Richard Clayton, and Alastair R. Beresford. "1000 days of UDP amplification DDoS attacks". In: *Proceedings of the APWG Symposium on Electronic Crime Research*. 2017.