DDoS 3.0 - How terrorists bring down the Internet

Aiko Pras, José Jair Santanna, Jessica Steinberger and Anna Sperotto

University of Twente
Enschede, The Netherlands
a.pras@utwente.nl, j.j.santanna@utwente.nl, jessica.steinberger@h-da.de, a.sperotto@utwente.nl

Abstract. Dependable operation of the Internet is of crucial importance for our society. In recent years Distributed Denial of Service (DDoS) attacks have quickly become a major problem for the Internet. Most of these attacks are initiated by kids that target schools, ISPs, banks and web-shops; the Dutch NREN (SURFNet), for example, sees around 10 of such attacks per day. Performing attacks is extremely simple, since many websites offer "DDoS as a Service"; in fact it is easier to order a DDoS attack than to book a hotel! The websites that offer such DDoS attacks are called "Booters" or Stressers", and are able to perform attacks with a strength of many Gbps. Although current attempts to mitigate attacks seem promising, analysis of recent attacks learns that it is quite easy to build next generation attack tools that are able to generate DDoS attacks with a strength thousand to one million times higher than the ones we see today. If such tools are used by nation-states or, more likely, terrorists, it should be possible to completely stop the Internet. This paper argues that we should prepare for such novel attacks.

1 Current DDoS attacks

Current DDoS attacks are often performed by youngsters via websites that offer "DDoS as a Service". Such websites, which are called "Booters" or Stressers", are able to generate attacks with strengths of many Gbps. A simple Google search shows that hundreds of such Booters are currently active; the costs to perform a series of attacks is typically a few dollars [1][2]. In general Booters do not attack their targets directly, but use one or two levels of intermediate systems to strengthen and anonymise the attacks. The first level is formed by botnets that start the attack once they receive specific commands from the Booter. The second level is used to amplify the attack and can, for example, involve a set of DNS or NTP servers that react upon the reception of relatively small requests by sending large response packets. The ratio between response and request message size is the amplification factor; in practice we find factors between ten and hundred. Particularly popular for amplification attacks are so-called open DNS resolvers, which are basically misconfigured DNS servers that answer DNS queries irrespective of their origin. To target a specific victim, the

attacker does not put its own IP-address in the request, but the address of the target. Response packets will therefore be routed towards the victim, and the identity of the attacker remains unknown (IP spoofing).

2 Analysis of current DDoS attacks

To understand how Booters operate, we will discuss a series of attacks which we performed on our own infrastructure [2]. Nine Booters were used; two of which generated so-called CharGen attacks whereas the other seven performed DNS amplification attacks. An interesting observation was that only two of these Booters shared their attack infrastructure. In other words, if an attacker would not use a single Booter but instead all available Booters, the strength of the combined attack would be nearly the sum of all individual attacks.

The strongest CharGen attack we performed had a strength of 7.5 Gbps, whereas the DNS amplification attacks varied in strength between 0.4 and 1.6 Gbps (Figure 1). Since CharGen attacks can easily be mitigated by filtering UDP port 19, in the remainder we will focus on DNS attacks, which are much harder to mitigate. Figure 2 shows the average DNS response message size for each Booter attack; for three of them the size remains below thousand bytes, whereas the three top Booters showed average sizes between 3000-4000 bytes. These differences can be explained from the fact that the various Booters queried different DNS host names. If the Booters that performed the weakest attacks would just change these host names, their attacks would become a factor three to four more powerful. Such changes can be implemented within a few seconds by just modifying a single line in the attack source code.

Finally we observed that each booter used between 3000 to 8000 DNS resolvers for amplifying the DNS attack. It should be clear that the strength of the attacks can easily be increased by using far more DNS resolvers.

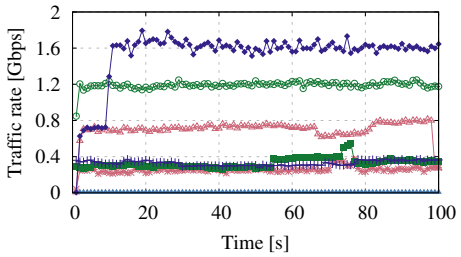

Fig. 1: DNS traffic rate

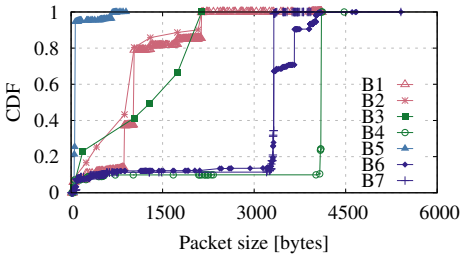

Fig. 2: DNS packet size distribution

We may conclude that DDoS attacks can easily be made stronger if 1) youngsters combine the forces of different Booters, 2) if Booter operators optimise their DNS queries and 3) more DNS resolvers are used.

3 How to make DDoS attacks more powerful

The interesting question is how a group of skilled "professionals" would proceed to generate attacks far beyond anything we've seen yet. Such "professionals" could be nation states or, more likely, a group of terrorists that aim at disrupting our current society. Instead of relying on standard Booters that operate under the control of some unknown entity, such "professionals" would likely build their own attack tools and infrastructure.

As opposed to Booters that use a limited set of 3000 to 8000 open DNS resolvers, "professionals" might use the potential of all existing open DNS resolvers to amplify attacks. According to the Open Resolver Project, around 20 million of such systems exist [3]. Alternatively, amplification can also be achieved by using standard authoritative DNS servers; there are hundreds of millions of such servers that allow amplification with a factors between 6 and 12. Particularly interesting may be the 3.5 million DNSSEC servers, which include digital signatures in their responses and therefore allow much higher amplification factors; factors between 40 and 55 should be realistic [4]. In addition to DNS systems, attackers can also use open NTP (4 million), open SNMP (8 million) or other servers to amplify attacks [5][6].

An important component is the botnet that coordinates and distributes the attack; the bigger the botnet, the more powerful the attack. An interesting question therefore is "how easy would it be to create a botnet with thousands of systems". One answer to this question can be found by examining the Carna Botnet that was created as part of the "Internet Census 2012" [7]. The creators of that botnet targeted access routers and other embedded devices running OpenWRT. They found 1.2 Million unprotected devices, of which 420 thousand were used for their Carna botnet. It took the developer(s) six months to develop the software and setup the infrastructure; once deployment started it took only a single day to infect the first 100 thousand systems.

Instead of hacking OpenWRT routers, "professionals" could also exploit the emerging Internet of Things (IoT) for their attacks. Recent reports by Garner and HP predicted that by 2020 there will be 26 billion active IoT devices, of which 60% will be insecure [8]. Even if only a fraction of them could be misused for DDoS attacks, it should be easy to generate attacks of hundreds of Tbps. If such attacks would target crucial systems, it is clear that the entire Internet would collapse with devastating consequences for our society .

4 Conclusions

In the previous section we argued that it is relatively easy to perform DDoS attacks with a strength thousand to one million times higher than the ones we see today. Such attacks can be launched by nation states or, more likely, terrorists. The question is not if massive DDoS attacks with a strength of hundreds of Tbps will take place, but when.

We should therefore prepare for such attacks, and create plans on how to react once such attacks take place. Like traditional terrorist attacks, governments

need to play a crucial role in the coordination of mitigation strategies; it is not acceptable to leave such role at Internet Service Providers (ISPs) or security companies. Governments should force ISPs to develop tools and techniques to automatically quarantaine customers with hacked devices that participate in massive DDoS attacks. ISPs should join forces and create "Trusted Networks" to ensure that some limited form of communication remains possible once such attacks take place.

Acknowledgments

This research is funded by FLAMINGO, a Network of Excellence project (318488) supported by the European Commission under its Seventh Framework Programme.

References

1. Chromik, J.J., Santanna, J.J., Sperotto, A., Pras, A.: Booter websites characterization: Towards a list of threats. In: Brazilian Symposium on Computer Networks and Distributed Systems (SBRC). (2015)
2. Santanna, J.J., van Rijswijk-Deij, R., Sperotto, A., Hofstede, R., Wierbosch, M., Granville, L.Z., Pras, A.: Booters - An Analysis of DDoS-as-a-Service Attacks. In: IFIP/IEEE International Symposium on Integrated Network Management (IM). (2015)
3. Website: Open Resolver Project. `http://openresolverproject.org` (2016)
4. v. Rijswijk-Deij, R., Sperotto, A., Pras, A.: DNSSsec and Its Potential for DDoS Attacks. Proceedings of the Fourteenth ACM Internet Measurement Conference **14** (2014) 449–460
5. Website: Open NTP Project. `http://openntpproject.org` (2016)
6. Website: Open SNMP Project. `http://opensnmpproject.org` (2016)
7. Website: Internet Census 2012 - the Carna Botnet. `http://internetcensus2012.bitbucket.org` (2012)
8. HP: Internet of things research study. Technical report, HP (2015)