# Bypassing DNS-based Traffic Diversion to Launch DDoS Attacks

Mattijs Jonker and Anna Sperotto

Design and Analysis of Communication Systems (DACS)
University of Twente
{m.jonker, a.sperotto}@utwente.nl

## ABSTRACT

Over the last years, Distributed Denial-of-Service (DDoS) attacks have rapidly gained in popularity. This simple yet very effective class of attacks can generate network traffic volumes of the order of hundreds of Gbps. As an example take the recent attack on *KrebsOnSecurity.com*, which reportedly reached a volume of *665 Gbps* [2]. Such high-volume attacks are nearly impossible to mitigate with strictly on-premise solutions, since these cannot prevent link saturation. To make matters worse, *Booters* nowadays offer DDoS attacks as a service, thereby allowing the layman to launch attacks in exchange for only a few USD. In the face of the increased threat of attacks, a market for DDoS Protection Services (DPS) was created, to which protection can be outsourced.

In recent work, we studied the worldwide adoption of DDoS Protection Services [1]. Our research was done on the basis of long-term, active Domain Name System (DNS) measurements, which allow us to determine if – and how – domains use a DPS for protection. Our data set consists of daily measurements, over a period of 1.5 years, for over 50% of all names in the global domain namespace, which includes the larger generic Top-Level Domains (gTLDs) .com, .net and .org, as well as the country-code TLD (ccTLD) .nl and Alexa's list of Top 1M Web sites. Our work not only confirms an increasing adoption of DPSs, but it also shows a trend that exceeds the overall growth in terms of new domain names. Moreover, our results show that adoption is not foremost driven by single users, but rather by larger parties such as Web hosters, which enable and disable protection for millions of domain names at once.

While outsourcing protection to a DPS is a viable option for protection, it knows various drawbacks, of which some relate to using the DNS to divert traffic to the security infrastructure of a DPS. A major drawback is caused by security by obscurity: the public IP address of a domain is obscured as its DNS zone is (re)configured for traffic diversion. Sometimes it is possible to determine the public IP on the basis of, e.g., a reference in an SPF record. If the origin IP of a Web site can be "unobscured", then protection can be circumvented and direct DDoS attacks can be launched [3].

With an open discussion at the DINR workshop we would like to identify novel vectors through which DNS-based traffic diversion can be circumvented. Such vectors can be added to a future measurement study, which will involve our large-scale and long-term data set of active DNS measurements.

## References

1. M. Jonker, A. Sperotto, R. van Rijswijk-Deij, R. Sadre, and A. Pras, “Measuring the Adoption of DDoS Protection Services,” in *To appear in Proceedings of the 2016 ACM Internet Measurement Conference (IMC'16)*. Santa Monica, CA, USA: ACM Press, 2016.
2. Brian Krebs. KrebsOnSecurity Hit With Record DDoS. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. Accessed: 2016-10-03.
3. Thomas Vissers, Tom van Goethem, Wouter Joosen, and Nick Nikiforakis. Maneuvering Around Clouds: Bypassing Cloud-based Security Providers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1530–1541, 2015.