Transparent DNS Forwarders: A (Still) Unnoticed Component of the Open DNS Infrastructure

Maynard Koch
TU Dresden
Dresden, Germany
maynard.koch@tu-dresden.de

Marcin Nawrocki
NETSCOUT
Germany
marcin.nawrocki@netscout.com

Thomas C. Schmidt
HAW Hamburg
Hamburg, Germany
t.schmidt@haw-hamburg.de

Matthias Wählisch
TU Dresden
Dresden, Germany
m.waehlisch@tu-dresden.de

EXTENDED ABSTRACT

The open DNS infrastructure (ODNS) [4] includes all devices that accept and resolve DNS queries from any client. As an open system, the ODNS infrastructure is a popular target for attackers who search for amplifiers of DNS requests, for periodic DNS scan campaigns, which try to expose the attack surface, and for researchers who want to learn more about DNS behavior.

Due to the danger posed by open DNS resolvers, *e.g.,* misusing them as amplifiers in DNS amplification attacks [1], several campaigns have been launched to raise awareness of open DNS infrastructure services. Their total number decreased from over 30 million in 2013 [4] down to only a few million devices nowadays. The two ODNS components that get most of the attention are recursive resolvers and recursive forwarders. However, there is also a third component called transparent forwarders, initially observed in 2013 [2]. These devices transparently relay DNS requests to (public) DNS resolver by spoofing the clients IP address.

Unfortunately, researchers and scanning campaigns paid little to no attention to transparent DNS forwarders. We recently revisited the open DNS (ODNS) infrastructure, systematically measured and analyzed transparent forwarders [3]. Our findings raised concerns for three reasons. First, the relative amount of transparent forwarders increased from 2.2% in 2014 to 26% in 2021 (and 31% in 2024). Second, as part of the ODNS, transparent forwarders interact with unsolicited, potentially malicious requests. Third, common periodic scanning campaigns such as Shadowserver or Censys still do not capture transparent forwarders and thus underestimate the current threat potential of the ODNS.

We argue that open transparent DNS forwarders pose a threat to the Internet infrastructure. To monitor the current state of the open DNS and better understand the deployment of transparent forwarders, we launched a long-term measurement campaign. We are currently in the process of extending support for multiple DNS transports, in addition to DNS over UDP and DNS over TCP. The results of this campaign are available on the following website:

https://odns.secnow.net/

In this presentation, we want to talk about our most recent findings on the ODNS infrastructure, in particular we will highlight insights gained between our initial study [3] and now. We will present our data set and would like to discuss potential collaborations to improve the current situation by reducing the amount of open transparent DNS forwarders.

Acknowledgments. We would like to thank Florian Dolzmann, Carl Bennet Kuhlmann, and Maximilian Stäps for providing the DNS over TCP implementation deployed on https://odns.secnow.net/.

REFERENCES

[1] Marios Anagnostopoulos, Georgios Kambourakis, Panagiotis Kopanos, Georgios Louloudakis, and Stefanos Gritzalis. 2013. DNS amplification attack revisited. *Computers & Security* 39, B (2013), 475–485. https://doi.org/10.1016/j.cose.2013.10.001

[2] Jared Mauch. 2013. Spoofing ASNs. NANOG mailing list. http://seclists.org/nanog/2013/Aug/132 Retrieved: May, 2021.

[3] Marcin Nawrocki, Maynard Koch, Thomas C Schmidt, and Matthias Wählisch. 2021. Transparent Forwarders: An Unnoticed Component Of The Open DNS Infrastructure. In *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies*. 454–462.

[4] Kyle Schomp, Tom Callahan, Michael Rabinovich, and Mark Allman. 2013. On Measuring the Client-Side DNS Infrastructure. In *Proc. of ACM IMC* (Barcelona, Spain). ACM, New York, NY, USA, 77–90. https://doi.org/10.1145/2504730.2504734