# Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path

## Baojun Liu

Tsinghua University/BNRist lbj15@mails.tsinghua.edu.cn

# Ying Liu

Tsinghua University/BNRist liuying@cernet.edu.cn

# Chaovi Lu

Tsinghua University/BNRist lcy17@mails.tsinghua.edu.cn

## Zhou Li

University of California, Irvine zhou.li@uci.edu

# Min Yang

Fudan University m yang@fudan.edu.cn

## Haixin Duan

Tsinghua University/BNRist duanhx@tsinghua.edu.cn

## Shuang Hao

University of Texas at Dallas shao@utdallas.edu

## **ABSTRACT**

DNS is a critical service for almost all Internet applications. DNS queries from end users are handled by recursive DNS servers for scalability. For convenience, Internet Service Providers (ISPs) assign recursive servers for their clients automatically when the clients choose the default network settings. On the other hand, users should also have the flexibility to use their preferred recursive servers, like public DNS servers. Since almost all DNS queries are sent in plain-text, it's possible for on-path devices to intercept DNS queries sent to public resolvers, by spoofing the IP addresses of user-specified DNS servers and surreptitiously responding using alternative resolvers instead. The trust relationship between users and public DNS are thus broken by the *hidden interception of the DNS resolution path* (which we term as DNS interception).

The hidden DNS interception can pose users to privacy and security threats, and we aim to shed light on this behavior in this study. It's challenging to observe DNS interception because we need vantages points distributed across the globe. We solved this problem by recruiting clients from a proxy network and popular security software with a large number of real-world users.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

ANRW '19, July 22, 2019, Montreal, QC, Canada © 2019 Copyright held by the owner/author(s). ACM ISBN 978-1-4503-6848-3/19/07. https://doi.org/10.1145/3340301.3341122

In this paper, we performed a large-scale analysis on onpath DNS interception and investigate its scope and characteristics. In practice, we designed a novel approach to detecting DNS interception and deployed a global measurement platform. Considering different transport protocols and various recursive servers, we have gained multi-faceted insights. In particular, using traffic from 148,478 residential and cellular IP addresses, we find that 259 of the 3,047 ASes (8.5%) that we inspect exhibit DNS interception behavior, including large providers, such as China Mobile. Particularly, 27.9% DNS/UDP queries from China to Google Public DNS are intercepted. Moreover, we find that alternative resolvers used by interceptors may use outdated software (which should be deprecated before 2009) and lack security-related functionality, such as handling DNSSEC requests. Our work highlights the issues around on-path DNS interception and provides new insights into its countermeasures.

Our research provides a first large-scale study on DNS end-to-end violation. Our work delivers evidence of DNS interception and serves as strong motivation of deploying encrypted DNS (e.g., DNS-over-TLS and DNS-over-HTTPS). After being published, our findings are reported by several well-known media, such as ACM Technews, The Register, and Hackread.

This paper is based on: Baojun Liu, Chaoyi Lu, Haixin Duan, Ying Liu, Zhou Li, Shuang Hao, and Min Yang. 2018. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path. In Proceedings of USENIX Security 2018. USENIX Security Symposium, Baltimore, USA, 16 pages. This work was supported in part by the National Natural Science Foundation of China (U1836213, U1636204) and the BNRist Network and Software Security Research Program (Grant No. BNR2019TD01004).

ANRW '19, July 22, 2019, Montreal, QC, RaojadaLiu, Chaoyi Lu, Haixin Duan, Ying Liu, Zhou Li, Shuang Hao, and Min Yang

## **CCS CONCEPTS**

• Security and privacy → Network security;

## **KEYWORDS**

DNS Security, DNS Interception, DNS Encryption

## **ACM Reference Format:**

Baojun Liu, Chaoyi Lu, Haixin Duan, Ying Liu, Zhou Li, Shuang Hao, and Min Yang. 2019. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path. In *ANRW '19: Applied Networking Research Workshop (ANRW '19)*, *July 22, 2019, Montreal, QC, Canada.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3340301.3341122