The Privacy Problems Behind RFC 7871 (Abstract)

Panagiotis Kintis*, Athanasios Kountouras*, David Dagon*, and Manos Antonakakis*

*Georgia Institute of Technology,
{kintis,kountouras,manos}@gatech.edu, dagon@sudo.sh

I. Introduction

The need for faster and more reliable access to Internet content is paramount. The Internet Engineering Task Force (IETF) and the "A Faster Internet" initiative [4] attempted to solve this problem by taking advantage of the distributed nature and reliability of DNS.

RFC 7871 [1] proposes a significant change in the information exchanged between a DNS Recursive (*recursive*) and Authoritative Nameservers (*authority*). According to RFC 7871, recursives that support the new EDNS Client Subnet (ECS) extension should include part of the client's IP address in the DNS packets they exchange with remote DNS servers. Clearly, the client-centric IP information in the DNS packets between the recursive and remote authorities will inevitably traverse various networks (likely in different Autonomous Systems) that the client's Layer 7 communications (i.e., HTTP/HTTPS sessions) might never go through.

This change in the DNS resolution process and the client information exchanged between the recursive and the authority, inevitably raise several privacy concerns [3]. In fact, Section 2 of RFC 7871, actually acknowledges the problem and states: "*Finally, we recommend that others avoid techniques that may introduce additional metadata in future work, as it may damage user trust.*".

II. Surveillance

Surveillance is a common method that nation states employ to monitor users' activity and behavior [2]. ECS makes such surveillance cases easier. It introduces more information in the DNS packets, that traverse the Internet, which can be easily obtained and analyzed by suppressing states. The IP address, or a part of it, that is contained in both the DNS questions and answers, can be extracted from the wire, when a packet is traveling through an Autonomous System (AS) that an adversary has access to.

In several cases, domain names are being hosted on shared infrastructure and the operation of the authority is being delegated to third parties. The authorities could reside in countries where regimes are able to identify not only the geographic location of visitors, but also more specific information, like the network they are coming from, their organization or even the identity of the user if ECS is configure to not mask the client's IP address.

III. Selective Cache Poisoning

In many cases DNS cache poisoning attacks are used when an adversary wants to take over a DNS zone and redirect users to a different host than the original one. Cache poisoning attacks have a global effect on clients around the world trying to resolve a domain name. ECS provides a new perspective to the attack, because of the nature of caching it supports.

For ECS enabled recursives, as ECS enabled responses are received, the recursives will cache such response for the particular ECS prefix. For example, a response that carries $\texttt{IP}_1$ in the "RDATA" field and $\texttt{CIDR}_1$ in the ECS payload, will only be cached for that specific prefix and will not be used when a client outside that network submits a resolution request. Therefore, a motivated adversary, can now inject a false Resource Record in a recursive's cache, without affecting any host, other than the targeted network, or even specific IP address.

Figure 1 shows an example of such attack. When a host submits a resolution request, someone on-path could passively monitor the network without interfering with the communication or even reveal her presence. Now, when a host from a targeted prefix network submits a resolution request, the packet that the recursive sends to the authority will contain the IP information of interest to a potential adversary. The adversary detects that network and injects a false DNS packet in the wire. From that point on, any response that the authority will submit will be dropped by the recursive and the bogus RDATA submitted by the adversary, will not be cached for that network only. An example of such attack and how he we rendered it can be found at https://youtu.be/U1ehqjGwETc.

IV. Conclusion

RFC 7871 provides a unique opportunity to improve the content delivery in Internet. However, it does not provide controls and procedures to preserve adequate level of security and privacy for the users. Mass surveillance opportunities and selective cache poisoning attacks are two of the potential new capabilities that adversaries will have and the security community will need to protect against.

References

[1] Carlo Contavalli, Wilmer Van Der Gaast, D. Lawrence, and W. Kumari. Client Subnet in DNS Queries. RFC 7871, May 2016.

[2] Electronic Frontier Foundation. Mass Surveillance Technologies. https://www.eff.org/issues/mass-surveillance-technologies, 2015.

[3] Panagiotis Kintis, Yacin Nadji, David Dagon, and Manos Antonakakis. Understanding the privacy implications of ecs. In *Detection of Intrusions and Malware, and Vulnerability Assessment: 13th International Conference, DIMVA 2016, San Sebastián, Spain, July 7-8, 2016, Proceedings*, volume 9721, page 343. Springer, 2016.

[4] OpenDNS. A Faster Internet: http://www.afasterinternet.com, 2011.

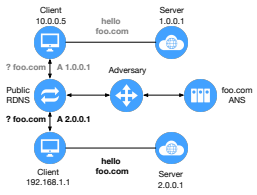

Fig. 1. Selective cache poisoning attack.