Explicit Forged Answer Signal

draft-pan-dnsop-explicit-forged-answer-signal-01

Lanlan Pan **Yu Fu(China Unicom)** Cuicui Wang(China Unicom)

draft-pan-dnsop-explicit-forged-answer-signal-01

- **Abstract**
  - This document describes about the forged answer provided by recursive resolver.
  - Client could protect user on security and privacy more efficiently **if recursive resolver gives explict signal in the forged answer.**

- **Background**
  - **Recursive resolver may make a forged answer for a dns query in some specific scenarios**
    - such as NXDOMAIN, phishing, fraud, malware, ransomware, botnet DDoS attack, and legal requirement, etc.
  - **The RCODE of faked answer is NOERROR,** which make client hard to distinguish it with honest answer, if client doesn't make iterative dns query by itself, or make DNSSEC validation.
  - Faked answer can avoid user to visit malicious website, however, it may also **increase the security and privacy risks**.

  Such as **HTTP Cookies Leakage**
    - Imagine that user visits "abc.example.com" in browser. Recursive resolver return a faked answer to browser.
    - Browser will visit the faked server, and leak the HTTP cookies in "example.com" of the user to it. With the leaked HTTP cookies, the faked server may pretend as the user to visit "abc.example.com", result in user's security issue and rivacy leakage.

draft-pan-dnsop-explicit-forged-answer-signal-01

- **Explicit Forged Answer Signal**

To avoid the HTTP cookies leakage, the recursive resolver is responsible for **giving explict forged answer signal to client**, and client could make its own reaction when it received an explict forged answer signal from recursive resolver.

- **Recursive Resolver**
  - Recursive resolver could give the explict forged answer signal by including an additional Extended DNS Errors (EDE) information in DNS response, which is defined in [RFC8914].
  - Alternatively, recursive resolver could include an TXT RR in DNS answer section, such as:

    abc.example.com 300 IN A 1.2.3.4

    abc.example.com 300 IN TXT "faked=malware"
- **Client**
  - Client could implement its own policy to deal with the forged answer:
    - **Use DNSSEC :**Client could make DNSSEC query by itself. If the domain has deployed DNSSEC, the client could validate the honest answer from authoritative server.
    - **Change Recursive Resolver:**Client could change to another recursive resolver which is not lying.
    - **Stop Visit:** Client could stop to visit on the website, since it knows that the answer is faked.
    - **Limited Visit:**Client could make limited visit on the website, prevent HTTP cookies from being send to the faked server. For example, browser should not send user's HTTP cookies to the faked server, if it gets an explict faked answer signal in the DoH response [RFC8484].