Structured Data for DNS Access Denied Error Page

draft-wing-dnsop-structured-dns-error-page-02

March 2022
IETF#113

D. Wing (Citrix)

T. Reddy (Akamai)

N. Cook (Open-Xchange)

M. Boucadair (Orange)
Purpose

• Parsable JSON for user and IT troubleshooting DNS filtering
• Client displays/logs the JSON with its own UI

• Updates to address comments
• Replaces draft-reddy-dnsop-error-page
Changes Since IETF#112

• Abandon the use of a new EDNS0 option to explain the reason for DNS filtering ...

• Instead, recast EXTRA-TEXT field in the EDE option for that purpose (updates RFC8914)
  ➢ Structured as JSON
JSON in EXTRA-TEXT Field

- JSON data in EXTRA-TEXT field of EDE option to explain the reason for DNS filtering

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-------------------------------------+  
0: |OPTION-CODE|  
+-------------------------------------+  
2: |OPTION-LENGTH|  
+-------------------------------------+  
4: |INFO-CODE|  
+-------------------------------------+  
6: /EXTRA-TEXT.../  
+-------------------------------------+  
```

JSON Attributes
(Variable Length)
Security Considerations

• Key updates:
  ➢ Encrypted resolver has sufficient reputation (e.g., TRR).
  ➢ Isolated environment to process the “c” and “r” pages (like captive portals)
    ➢ Label the page as untrusted
    ➢ Prevent user interaction
    ➢ Prevent transmitting cookies, block JavaScript, block auto-fill of credentials or personal information, and be isolated from the user's normal environment

• (Non-Exhaustive) Security Cons
  ➢ Encrypted and Authenticated DNS connection is mandatory.
  ➢ Many others in the draft.
Next Steps

• Addressed all the comments from the WG
• Consider for WG adoption
An Example of Supplied Data

```json
{
    "c": "?time=1621902483", // Used to report a misclassified filter
    "d": "ns.example.com", // FQDN of the encrypted server
    "j": "malware present for 23 days", // Justification
    "o": "example.net Filtering Service", // Organization responsible for the filtering
    "r": "?country=atlantis" // Regulation
}
```

https://ns.example.com/?time=1621902483&type=a&name=malware.com

Blocked Domain