Local DNS Policy Disclosure

“Comments on Automating Policy Discovery”

David Dagon
May 13, 2019
Context

- **Caveat:** This is replacement talk
- DNS Filtering perspectives: SOPA/PIPA (Background discussion)
Previously on google.com...

Millions of Americans oppose SOPA and PIPA because these bills would censor the Internet and slow economic growth in the U.S.

Two bills before Congress, known as the Protect IP Act (PIPA) in the Senate and the Stop Online Piracy Act (SOPA) in the House, would censor the Web and impose harmful regulations on American business. Millions of Internet users and entrepreneurs already oppose SOPA and PIPA.

The Senate will begin voting on January 24th. Please let them know how you feel. Sign this petition urging Congress to vote NO on PIPA and SOPA before it is too late.
● DNS Filtering perspectives: SOPA/PIPA
● With DOH (and DNSSEC, ECS, etc.) we have new resolution policy issues
● Countless DNS-filtering tools and policy appliances:
  ● Many paid for and/or installed by user or site administrator
  ● Many opaque and inherent in network access agreements
  ● Many illicit or imposed
● Reviewing a few reveals trends
https://dsi.ut-capitole.fr/blacklists/index_en.php

“Be careful : this list should not be seen as a 'to be block'. It must be seen as a 'web categorization' : some categories can be blocked or allowed, depending on your environnement.”

**Contexte**

The Université Toulouse 1 Capitole propose a blacklist managed by Fabrice Prigent from many years, to help administrator to regulate Internet use. This database, often used in school, can be used with many commercial or free software.

Be careful : this list should not be seen as a "to be block". It must be seen as a "web categorization" : some categories can be blocked or allowed, depending on your environnement.

**Licenses**

Contrat Creative Commons
This creation is available under un Creative Commons Contract.

**Description**

Many categories are defined, but It's the main one is "pornography".

When a category is defined, the other ones is also defined.
DNS Filtering Service

A DNS filtering service is an alternative to more traditional hardware and software-based solutions for filtering the Internet. A DNS filter works by redirecting the IP address of an organization’s router to that of the service provider and then allowing administrators to set the filtering parameters via an online browser-based portal.

Because a DNS web filtering service is quick to implement, has low maintenance overheads and is inexpensive to operate, it is quickly becoming the “go to” solution for organizations wanting to increase their online security postures and protect their networks from web-borne threats. A DNS filtering service has other benefits for organizations as well.

The Importance of a DNS Filtering Service with SSL Inspection

SSL inspection is a tool within a DNS filtering service that decrypts the content of a “secure” website, checks the content for its integrity, and then re-encrpyts the website before allowing an Internet user access to the site. The reason why SSL inspection is so important is because three-quarters of websites use encrypted connections to protect the privacy and integrity of the user’s data.
Consent

- Existing repositories of DNSBL data
- TODO: survey policy transparency
  - Excellent resource https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Reference+Material
- Key to legitimacy: *Informed user consent*
- Policy transparency: the ability of end users to discover rules, limits, protections, and options.
  - Not a new concept
  - 2002 ePrivacy Directive (Cookie Law)
  - GDPR: User control of data
  - And misc laws, policies in US, CA, elsewhere
Short Idea

- Perhaps a neutrally operated global zone, such as example.com or icann.org, or dnspolicy.arpa, could be instrumented with child labels that DNS filtration tools {may, should, will} edit to exhibit user policy choice.
  - E.g., IN A? $NONCE.dnspolicy.arpa, global wildcard returns NXDOMAIN. DNS filters adjust RCODE=0.
  - Perhaps indicated RDATA offers local policy guidelines (or 127/8 if none etc.)
  - Other behavioral labels:
    - refused.dnspolicy.arpa, SHOULD globally and locally returns RCODE=5
    - nxdomain.dnspolicy.arpa, SHOULD globally and locally returns RCODE=3
- Policy choices thereby optionally disclosed to the browser (FP vs FN trade off)
- DOH UI selection may address this proof of DNS policy.
Existing DNS/RDATA Policy Checks and Behaviors

- RFC 2606, RFC 6761: .example, .localhost, etc.
- Also example.com, etc., devoid of meaningful L7, for leak-free docs
- Similarly, constoso.com is "globally local", and used for MS training/documentation
- Chrome 3x random HEAD requests, detecting NXDOMAIN rewriting, "error path correction", and DNS hijacking
- The IANA operated pTLD list contains zone data for roots, some such as .onion with policy instructions (e.g., RCODE=5, do not iterate, etc.)
Why REFUSED child entry?

- Users have mixed resolution paths: filter/no-filter
- Informed consent requires transparency in all paths

  - **Avoidance of unresponsive DNS servers**

    The DNS Client service uses a server search list, ordered by preference. This list includes all preferred and alternate DNS servers configured for each of the active network connections on the system.

    The list is arranged based on the following criteria:

    1. Preferred DNS servers are given first priority.
    2. If no preferred DNS servers are available, then alternate DNS servers are used.
    3. Unresponsive servers are removed temporarily from these lists.

https://docs.microsoft.com/en-us/\previous-versions//cc977482(v=technet.10)

https://docs.microsoft.com/en-us/\previous-versions/windows/it-pro/\windows-server-2003/cc779517(v=ws.10)
The AV industry uses a non-malicious string for testing.

The EICAR test string reads:

X501P%@AP{4\PZ54(P*)7CC}7$EICAR-STANDARD-ANTIVIRUS-TEST-FILE$\H*

NOTE: The third character is the capital letter 'O', not the digit zero.

Hash values
(Hashed with trailing newline character)

<table>
<thead>
<tr>
<th>Hash type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC32</td>
<td>1dd02bdb</td>
</tr>
<tr>
<td>MD5</td>
<td>69630e4574ec6798239b091cda43dca0</td>
</tr>
<tr>
<td>SHA1</td>
<td>cf8bd9dfddff007f75adf4c2be48005cea317c62</td>
</tr>
<tr>
<td>SHA224</td>
<td>a2e3aa5b00d6b05643f99e619c2d16deef927d171861477696be5b4c0</td>
</tr>
<tr>
<td>SHA256</td>
<td>131f95c51cc819465f01797f6ccacff9d494a44f46fa3ea3193e6d3fbbd68d267</td>
</tr>
<tr>
<td>SHA384</td>
<td>10cc0011d21012867900a17757c239025dac46589f8e08e93916d773a1dcc6257b357e408112d09f95c9d3401d25700</td>
</tr>
<tr>
<td>SHA512</td>
<td>5581f85b25f0d80fe84c69e7ca24d98344f5fbaec45b7707dcc139a8c665961391d6e762516e1db3137c4d82eaca7fbc67c348c37ea0d67bb88161cf3b3008</td>
</tr>
</tbody>
</table>
Chrome does 3x random HEAD requests. See master/chrome/browser/intranet_redirect_detector.cc

```cpp
// Start three loaders on random hostnames.
for (size_t i = 0; i < 3; ++i) {
    std::string url_string("http://");
    // We generate a random hostname with between 7 and 15 characters.
    const int num_chars = base::RandInt(7, 15);
    for (int j = 0; j < num_chars; ++j)
        url_string += ('a' + base::RandInt(0, 'z' - 'a'));
    GURL random_url(url_string + '/');

    auto resource_request = std::make_unique<net::ResourceRequest>();
    resource_request->url = random_url;
    resource_request->method = "HEAD";
}
```

Often confused as malicious (by design)
Cf: Contoso

Microsoft’s testing company.

https://docs.microsoft.com/en-us/microsoft-365/enterprise/contoso-overview

Overview of the Contoso Corporation
09/13/2018 • 2 minutes to read • Contributors

Summary: Understand the Contoso Corporation as a business and the tiered structure of its worldwide offices.

The Contoso Corporation is a multi-national business with headquarters in Paris, France. It is a conglomerate manufacturing, sales, and support organization with over 100,000 products.

Contoso around the world

Figure 1 shows the headquarters office in Paris and regional hub and satellite offices in various continents.
Reminder: DOH will amplify what is today merely a few leaks
Benefits of SUDN Policy Domain

- Incentives for policy transparency
- Browsers should accept/believe/report voluntary filter disclosures—but doubt denials.
- Perhaps less “pollution” of nTLDs, assuming Chrome learns enough in initial *.dnspolicy.arpa resolutions
  - Less noise in malware detection!
- DNS filtering tools motivated to adopt: Preserves user base post-DOH
- Theory: Censors and malicious DNS editors not rewarded; likely agnostic?
  - Users likely gain a diagnostic tool of limited value
  - User testing likely identical to mere browser starting
  - Consultation needed with domain experts
Local policy represents intentional user choice or rules.
UI contexts should reference it, specifically.
Further Considerations

- Verification of dnspolicy.arpa site data?
  - How to render policy page? Safety? TLS?
  - Perhaps DNSSEC sign the test zone. (cf. dnssec.fail)
  - e2e DNSSEC incentive!

- FP low, FN likely still high

- Localization of policy document to LAN?

- Neutrality of testing zone (cf. ASN 112)

- Likely technologically neutral viz. ad-ware blockers and advertisers?
Credits and Caveats

• Utility of dnspolicy.arpa, and hosting of policy content from others. (Thanks!)

• Thanks to several anonymous attendees offering comments

• Idea offered to stimulate debate
Resolver Information Self-Publication

- [https://tools.ietf.org/html/draft-sah-resolver-information-00](https://tools.ietf.org/html/draft-sah-resolver-information-00)
- Sood, Arends and Hoffman
- Resolvers self-publish if they perform DNSSEC
- SUDN and RRTYPE: resolver-info.arpa/IN/RESINFO and well-known URI
- I-JSON response (RFC 7493), only from Recursives
- Json response has inventory field, plus TBD
- ‘‘If the resolver understands the RESINFO RRtype, the RRset in the Answer section MUST have exactly one record’’
- Structured

- Thus, “policy filtering awareness” could be a json field
<table>
<thead>
<tr>
<th></th>
<th>SUDN &amp; A?</th>
<th>SUDN &amp; RESINFO? &amp; .wellknown</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>policy format</strong></td>
<td>wildwest</td>
<td>I-JSON</td>
</tr>
<tr>
<td><strong>adoption</strong></td>
<td>trivial</td>
<td>RRType Tax</td>
</tr>
<tr>
<td><strong>scope</strong></td>
<td>RD=1 policy only</td>
<td>RD=1 policy &amp; DNSSEC &amp; ...</td>
</tr>
<tr>
<td><strong>paths</strong></td>
<td>multi-path</td>
<td>Unclear</td>
</tr>
<tr>
<td><strong>DDoS/Amp</strong></td>
<td>Merely IN A?</td>
<td>Filterable</td>
</tr>
</tbody>
</table>
Open Issues

- Good precedence for “testing/metadata” centric zone
- How to prevent policy transparency devolving into an ad? (Yaml response?)
- What about split policies? (One /etc/resolv.conf entry filters, the other is quad 9?)
- Can policy fields be enumerated into categoricals?
Comments Seem Likely