NXNSAttack対策で引けなくなったドメイン名

株式会社
インターネットイニシアティブ
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

ある日・・・

5/21: NXNSAttack disclose

5/2X: キャッシュDNSサーバの両系アップデート完了

6/0X: 回線サービスのサポート担当からエスカレーション

「お客様が名前解決できないドメイン名があるとおっしゃっているのですが、調べてみたんですけどSERVFAILになる理由がわからなくて…」

私「ほうほう？」

問題のドメイン名

tile.openstreetmap.org.

- **たしかに、IIJのキャッシュDNSサーバに聞くとSERVFAILになる**
- **dig +traceすると引ける**

```
openstreetmap.org. 86400 IN NS daisy.ns.cloudflare.com.
openstreetmap.org. 86400 IN NS rajeev.ns.cloudflare.com.
;; Received 98 bytes from 2001:500:f::1#53(2001:500:f::1) in 172 ms

tile.openstreetmap.org. 86400 IN CNAME tile.geo.openstreetmap.org.
geo.openstreetmap.org.  86400 IN NS chrysophylax.openstreetmap.org.
geo.openstreetmap.org.  86400 IN NS katie.openstreetmap.org.
geo.openstreetmap.org.  86400 IN NS saphira.openstreetmap.org.
geo.openstreetmap.org.  86400 IN NS stormfly-04.openstreetmap.org.
geo.openstreetmap.org.  86400 IN NS ridgeback.openstreetmap.org.
geo.openstreetmap.org.  86400 IN NS balerion.openstreetmap.org.
;; Received 205 bytes from 173.245.58.90#53(173.245.58.90) in 6 ms
```

問題のドメイン名

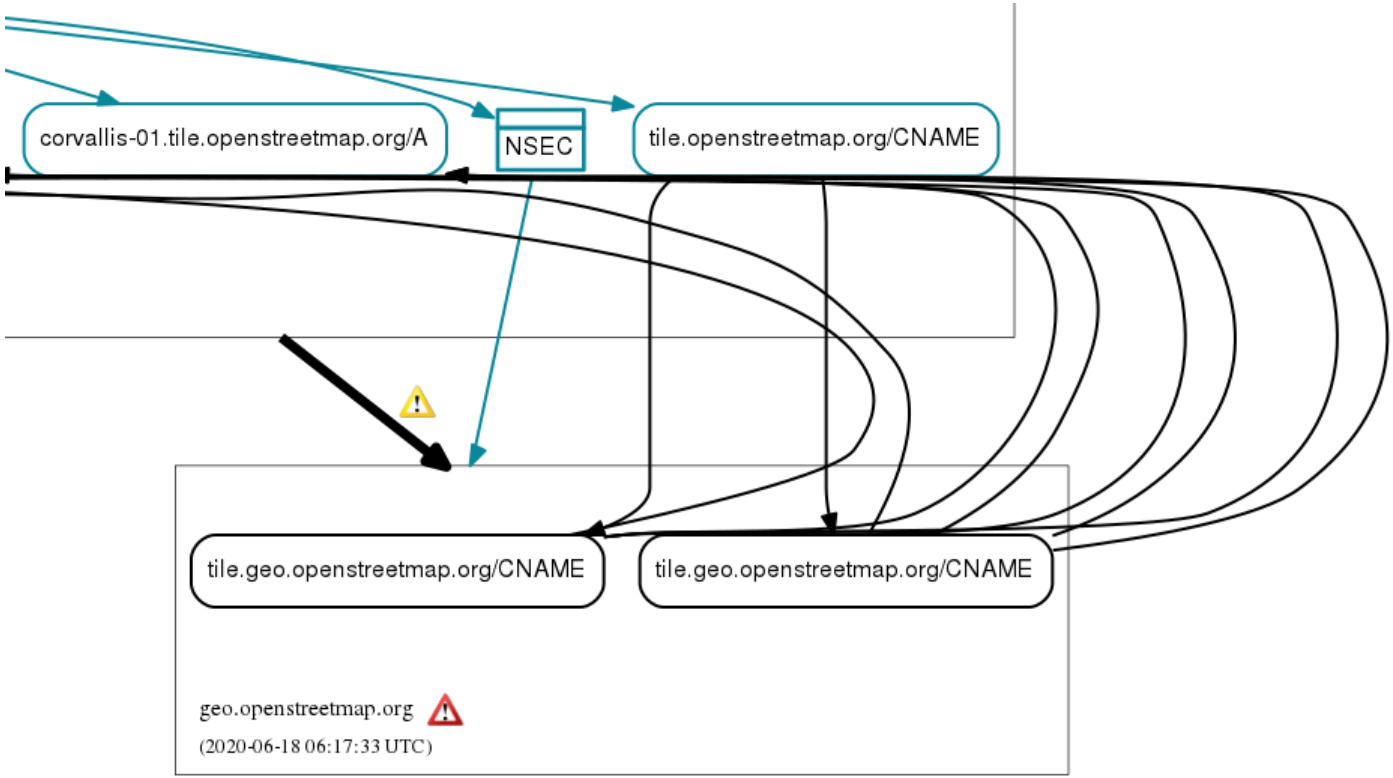
```
tile.geo.openstreetmap.org. 600 IN CNAME hsinchu.tile.openstreetmap.org.
;; Received 71 bytes from 2001:8e0:40:2039::10#53(2001:8e0:40:2039::10)
   in 203 ms

hsinchu.tile.openstreetmap.org. 600 IN A 140.110.240.7
;; Received 64 bytes from 2606:4700:50::adf5:3a5a#53(2606:4700:50::adf5:
   3a5a) in 2 ms
```

- 「8.8.8.8では引けるんですよね」あるあるあるあるあ

比較してみる

・手元にbuildしてあった、unbound-1.8.x: 引ける
・手元でbuildした、unbound-1.10.1: 引ける
あれぇー…？
→ ところが、しばらく時間が経ったら引けなくなった
ちなみに、1.8.xでは時間が経っても引ける
→ つまり、キャッシュの状態に依存しているっぽい

dnsviz.netで調べてみる



https://dnsviz.net/d/tile.openstreetmap.org/XusG_A/dnssec/

dnsviz.netでのエラー

Errors:

geo.openstreetmap.org zone: The following NS name(s) did not resolve to address(es): [a-f].ns.openstreetmap.org

Warnings:

openstreetmap.org to geo.openstreetmap.org:
The following NS name(s) were found in the authoritative NS RRset, but not in the delegation NS RRset (i.e., in the openstreetmap.org zone): [a-f].ns.openstreetmap.org

openstreetmap.org to geo.openstreetmap.org:
The following NS name(s) were found in the delegation NS RRset (i.e., in the openstreetmap.org zone), but not in the authoritative NS RRset: balerion.openstreetmap.org, …

geo.openstreetmap.org NS

ん？ [a-f].ns.openstreetmap.org…？？

```
dig @daisy.ns.cloudflare.com -t ns geo.openstreetmap.org

;; ANSWER SECTION:
geo.openstreetmap.org. 86400 IN NS saphira.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS ridgeback.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS balerion.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS katie.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS stormfly-04.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS chrysophylax.openstreetmap.org.
```

geo.openstreetmap.org NS

ん？ [a-f].ns.openstreetmap.org…？？

```
dig @balerion.openstreetmap.org –t ns geo.openstreetmap.org

;; ANSWER SECTION:
geo.openstreetmap.org. 86400 IN NS a.ns.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS b.ns.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS c.ns.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS d.ns.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS e.ns.openstreetmap.org.
geo.openstreetmap.org. 86400 IN NS f.ns.openstreetmap.org.
```

移譲元と移譲先で応答が異なる。そして、
“[a-f].ns” これら全てでA/AAAAが存在しない！

そういえば

Unbound-1.8.x: 時間が経っても名前解決できる

Unbound-1.10.1: 時間が経つと名前解決できなくなる

むむむ…これは……

log levelをあげて(verbosity: 3)みる

```
Level 1 gives operational information.
Level 2 gives detailed operational information.
Level 3 gives query level information, output per query.
Level 4 gives algorithm level information.
Level 5 logs client identification for cache misses.
```

Unboundのログ

1.10.1:

1. X.nsのA/AAAAを移譲元の示す、geoのNS全台に順番に聞きに行く → NXDOMAIN
2. 〃 移譲元のNSに聞きに行く → NXDOMAIN
3. [a-f].ns全てに関して1-2を試行する(6回) → すべてNXDOMAIN

⇨

```
debug: request has exceeded the maximum  number of
       nxdomain nameserver lookups with 6
debug: return error response SERVFAIL
```

むむっ…！

sourceを見てみる

https://github.com/NLnetLabs/unbound/blob/master/iterator/iterator.c#L2181

```
2181        if(iq->target_count && iq->target_count[2] > MAX_TARGET_NX) {
2182                verbose(VERB_QUERY, "request has exceeded the maximum "
2183                        " number of nxdomain nameserver lookups with %d",
2184                        iq->target_count[2]);
2185                errinf(qstate, "exceeded the maximum nameserver nxdomains");
2186                return error_response(qstate, id, LDNS_RCODE_SERVFAIL);
2187        }
```

https://github.com/NLnetLabs/unbound/blob/master/iterator/iterator.h#L60

```
60  /** max number of nxdomains allowed for target lookups for a query and
61   * its subqueries */
62  #define MAX_TARGET_NX          5
```

匂う…これはもしや…

NXNSAttack対応Patchを見てみる(git blameでも)

https://github.com/NLnetLabs/unbound/blob/master/iterator/iterator.h

```
@@ -2136,6 +2178,13 @@ processQueryTargets(struct module_qstate* qstate, struct iter_qstate* iq,
                errinf(qstate, "exceeded the maximum number of sends");
                return error_response(qstate, id, LDNS_RCODE_SERVFAIL);
        }
+       if(iq->target_count && iq->target_count[2] > MAX_TARGET_NX) {
+               verbose(VERB_QUERY, "request has exceeded the maximum "
+                       " number of nxdomain nameserver lookups with %d",
+                       iq->target_count[2]);
+               errinf(qstate, "exceeded the maximum nameserver nxdomains");
+               return error_response(qstate, id, LDNS_RCODE_SERVFAIL);
+       }
```

ですよねーー

というわけで、NXNSAttacck対策で一度の名前解決中のNXDOMAINの回数に上限(5回まで)が設けられたためでした。しかも、丁度良く(?)6個のNSという…。5個までだったら引き続き大丈夫だった。

before NXNSAttack対策の挙動

というか、NXDOMAINの回数上限に当たっていない場合

3. [a-f].ns全てに関して1-2を試行する→ すべてNXDOMAIN
4. **移譲元のNS(cloudflare)にtile.geo.openstreetmap.org Aを聞く (へぇー…)**
5. referralで返ってきたNS(saphira等。名前解決できる)に対して
   tile.geo.openstreetmap.org Aを聞き
   CNAME hsinchu.tile.openstreetmap.org を得る
6. hsinchu.tileのAをopenstreetmap.orgのNS(cloudflare)に聞き、Aを得る

不明点

- 手元だとtile/tile.geoのTTLが切れた直後はSERVFAILになるが、その直後に引くと名前解決できる。以後平気
  - ⇨ infra cacheが効いているから？
    - ⇨ unbound-control flush_infra allしても名前解決できる。なんで？

不明点

・本番環境だとSERVFAILになり続ける。configが同じでも差異が生じる。

⇨ 流量の違い？

⇨ 殆ど使われてない本番サーバでも発生する

初回のSERVFAIL後、geoのNSのTTL経過後、一度名前解決成功し、その後tile/tile.geoのTTLが切れるとまたSERVFAILになる