jp.sharp について

IIJ
Internet Initiative Japan

IIJ/DNSOPS.jp幹事
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

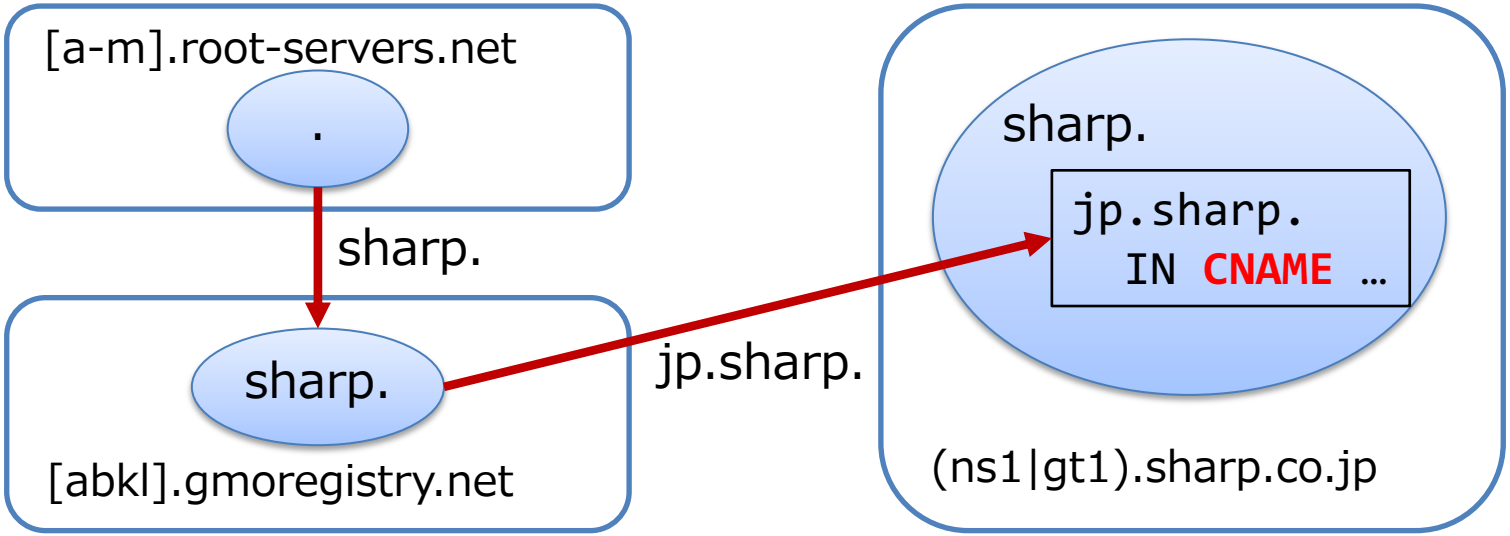
なにが起こった？

10/22 時刻不明(少なくとも17時以前)～10/27 19時頃？

~~**マスクが買えねーぞ (#°Д°)ｺﾞﾙｧ!!**~~

jp.sharp が名前解決できません！

構成の推測



構成の推測

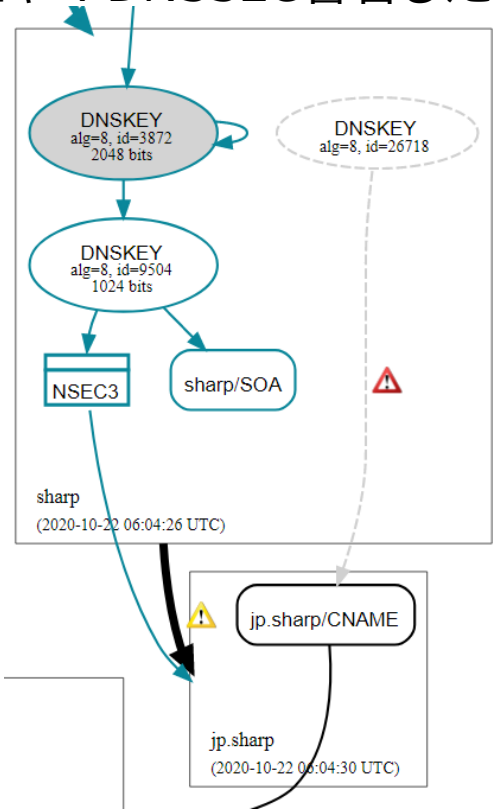
問題発生前、及び復旧後

```
$ORIGIN sharp.

@    IN SOA …

@    IN NS ns1.sharp.co.jp.
@    IN NS tg1.sharp.co.jp.

jp   IN CNAME ualsharp.hs.llnwd.net.
```

zone apexにCDNを被せたい…(CNAME書きたい) 「あるあるあるある」
でも、zone apexにCNAMEは書けない…。
せや！親ドメインでzone cutすればええやろ！

問題発生時

せや！DNSSEC署名したろ！！



RRSIG jp.sharp/CNAME alg 8, id 26718: The Signer's Name field of the RRSIG RR (sharp) does not match the name of the zone containing the RRset (jp.sharp).

```
$ORIGIN sharp.

@    IN SOA …

@    IN NS ns1.sharp.co.jp.
@    IN NS tg1.sharp.co.jp.

jp   IN CNAME ualsharp.hs.llnwd.net.
jp   IN RRSIG CNAME …
```

はて…？

RRSIGは追加されたが、対応するDNSKEYがない。
しかし、上位ゾーンにDSの登録もない。

…あれ？これってbogus(SERVFAIL)になるの…？

⇨ BIND, PowerDNS recursor, Knot resolverではならない。
　UnboundはbogusになるUnboundはbogusになる

う、うーん…

⇨ tss先生がunbound-usersに突撃するも、碌な応答がない

RFC的にはどうなるべきなの？ 教えて！詳しい人！！

ちなみに

(新g?)TLDのzoneにはCNAMEレコード書いてはいけないらしいです

1. DNS Service – TLD Zone Contents

Notwithstanding anything else in this Agreement, as indicated in section 2.2.3.3 of the gTLD Applicant Guidebook, permissible contents for the TLD's DNS service are:

1.1. For the "Internet" (IN) Class:

1.1.1. Apex SOA record

1.1.2. Apex NS records and in-bailiwick glue for the TLD's DNS servers

1.1.3. NS records and in-bailiwick glue for DNS servers of registered names in the TLD

1.1.4. DS records for registered names in the TLD

1.1.5. Records associated with signing the TLD zone (e.g., RRSIG, DNSKEY, NSEC, NSEC3PARAM and NSEC3)

1.1.6. Apex TXT record for zone versioning purposes

1.1.7. Apex TYPE65534 record for automatic dnssec signing signaling

thanks JPRS 阿波連さん

https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf#page=40

どうしていればよかったのか？

そもそも、ちゃんとRRSIGとDNSKEYをセットで登録する

1. CNAME Flattingに対応した権威DNS(サービス)
2. HTTPS (Type65) RR
   日本語解説: HTTPSの接続情報を通知する “HTTPS DNSレコード” の提案仕様
   まだ使われはじめの段階

```
@ IN HTTPS 0 cdn.example.com.
```

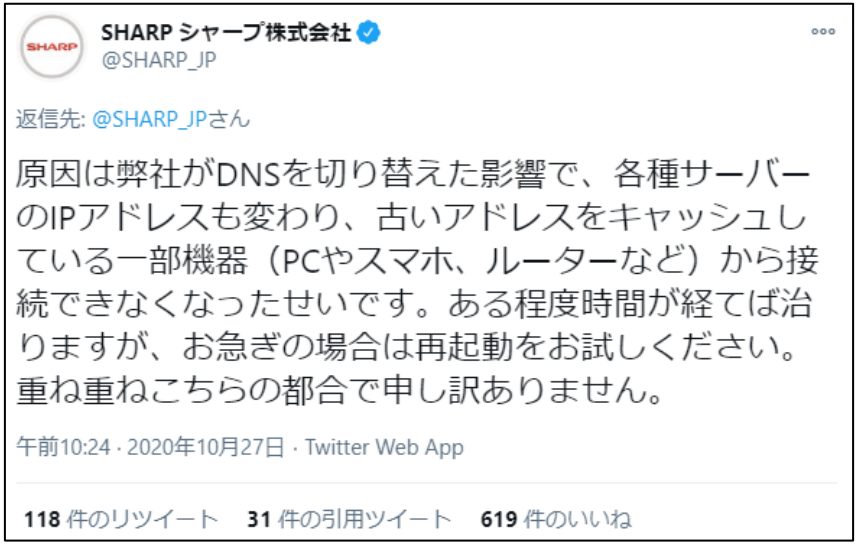
- iOS 14
- Chrome
  - 手元のWindows, Linuxでは確認できず
  - フルサービスリゾルバには結構な割合来ている
    A: 57% AAAA: 29% HTTPS: 12%

そもそも

zone apexにCNAMEは書けない事になっているけど、
書くとどんな実害が生じるの？(つぶら

教えて！詳しい人！！

ところで



SHARP シャープ株式会社
@SHARP_JP

返信先: @SHARP_JPさん

原因は弊社がDNSを切り替えた影響で、各種サーバーのIPアドレスも変わり、古いアドレスをキャッシュしている一部機器（PCやスマホ、ルーターなど）から接続できなくなったせいです。ある程度時間が経てば治りますが、お急ぎの場合は再起動をお試しください。重ね重ねこちらの都合で申し訳ありません。

午前10:24 · 2020年10月27日 · Twitter Web App

118 件のリツイート　**31** 件の引用ツイート　**619** 件のいいね

ウェブサイト接続障害のお知らせ

2020年10月27日

現在、一部の環境において、当社ウェブサイトに接続できないという障害が発生しております。
原因は、当社ウェブサーバー構成の変更に伴い、インターネットにおける名前解決情報の反映に時間がかかっているためと想定しており、時間の経過とともに解消される見込みです。
なお、閲覧に利用される機器の、Wi-Fi機能OFF/ON、本体の再起動で解消する場合がございます。
ご迷惑をおかけして誠に申し訳ございませんが、しばらくお待ちいただきますよう、お願い申し上げます。

SAD DNSについて

IIJ
Internet Initiative Japan

IIJ/DNSOPS.jp幹事
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

大元と参考サイト

https://www.saddns.net/

SAD DNSのICMP rate limitを用いた
サイドチャネル攻撃について - knqyf263's blog
https://knqyf263.hatenablog.com/entry/2020/11/19/200900

このスライドは8割knqyf263氏のblog記事をまとめただけです
最後に疑問点を書いていますが。

~~3~~ 4行で

新しいDNS Cache poisoning手法
DNS応答パケットのエントロピー:
　TXID(2^16) * source port数(65535-1024) ≈ 2^32
source port番号を推測(同定)することで、エントロピーを2^16+2^16 (=2^17) に下げられる

推測方法: ICMP port unreachableと、そのrate limitを利用
　(サイドチャネル攻撃)

source portの推測方法 (1)

1. **空いてないportにUDPパケットを投げつけるとICMP port unreachableが返る**

   しかし、これにはrate limitがかかっていて、Linuxではデフォルト50packet/20msec

2. **20msec以内に、ばらばらのsrc IPで、50個の異なるdst portにパケットを投げる (rate limit上限に達する)**
3. **その後、攻撃者のsrc IPで確実に閉じてるであろうdst portにパケットを投げる**

   ⇨ **port unreachが返ってこない → 50個全部閉じている**

   port unreachが返ってくる → 50個の中に空いているportが1つはある

source portの推測方法 (2)

あとは二分探索などをする

1秒で1000port程度scan可能

→ 65535-1024 スキャンするのに64.5秒かかる

スキャン中に正規の権威DNSサーバからの応答パケットが届いてしまうと、おじゃん。

フルサービスリゾルバのクエリを送出しているIPアドレスをsrc IPとして(偽装) 、正規権威DNSサーバに大量にクエリを送る

正規権威DNSサーバはRRLを発動させて、応答を一定割合で破棄する → 応答の遅延を引き起こし、その間を狙う

影響

みんな大好きRHEL/CentOSでは

- **6: global rate limitがないので影響なし**
- **7: 3.10系だが影響あり 8: 影響あり**

What versions of the operating system were affected?

- *Linux 3.18-5.10* ⇦ 5.9だと思う
- *Windows Server 2019 (version 1809) and newer (*)*
- *macOS 10.15 and newer (*)*
- *FreeBSD 12.1.0 and newer (*)*

**: we did not test older versions*

対策

DNSSEC (SERVFAILは…)

dns0x20

DNS Cookie

送信側のICMP port unreachableを無効化(遮断)

ICMP(v6)を全部遮断してはダメです (とくにIPv6)

ICMP port unreachableのrate limitのランダム化

Linux 5.10にて導入 (まだRC…)

疑問点

「RRLによって権威DNSサーバの応答が来る前にsource portを推測して、偽の応答を送りつけることが可能」って本当に？

BINDのRRLの発動具合: (初期実装で、今は違う可能性あり)

- 設定値を超える割合でresponseを返す場合、半分はdropし、半分はTC bitをonにした応答を返す

TC bit onの応答パケットを受け取ったリゾルバのUDP portは閉じますよね…？

あと、source portわかっても、1packetで攻略できるわけではない(TXID: 2^16)ので、更に時間が必要

- 権威DNSをDDoSなどで落として、全く応答が返ってこないのなら、じっくり料理可能

疑問点

ロス率50%でも、20回中9回は毒入れできた？

Table 3: Production Resolver Attack Results

Exp.	RTT range	Probe loss	Name sever mute level	Average time taken	Success rate
Base(D)	0.2-1.2ms	~0%	80%	504s	20/20*
Base(M)	0.2-1.2ms	~0%	80%	410s	20/20*
Mute Lv.	0.2-1.2ms	~0%	75%	1341s	18/20*
Mute Lv.	0.2-1.2ms	~0%	66.7%	2196s	20/20#
Mute Lv.	0.2-1.2ms	~0%	50%	8985s	9/20#
Altered	37-43ms	0.20%	80%	930s	5/5*

*: 1-hour threshold. #: 3-hour threshold. D: Day. M: Midnight

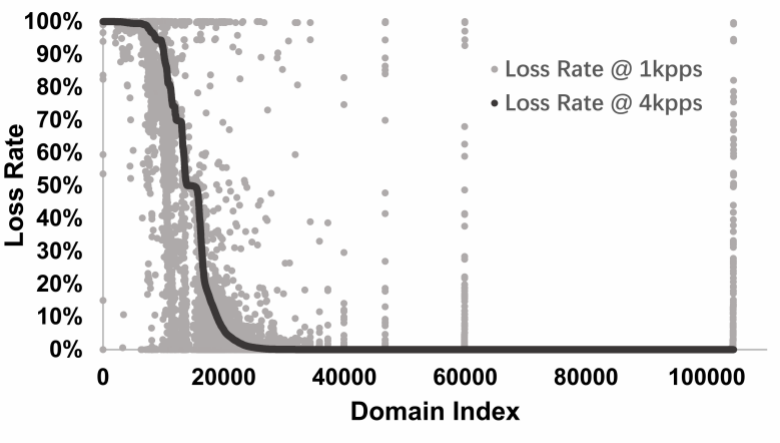


Figure 6: Response Loss Rate under Different Query Rate

「Alexa top 10kのうち、ロス率66.7%を超えたのは、1kppsで13%, 4kppsで18%もあったよ」？

DNS Flag Day 2020

IIJ
Internet Initiative Japan

IIJ/DNSOPS.jp幹事
島村 充
<simamura@iij.ad.jp>

Ongoing Innovation

なんだっけ？

IPフラグメンテーションアタックを喰らいにくいように、
ENDS Buffer sizeを1232byteに下げましょう

みなさん、やりました？