それでは、次は？

DNS Summer Day 2019, Tōkyō, 2019-06-28
Jan Hilberath / Open-Xchange

Stay Open.

DNS Flag Day とは?

モティベーション

- 2018年に、4社のオープンソース DNS ソフトウェアベンダーに開始
  - BIND, Knot, Unbound, PowerDNS
- DNS は複雑なので
  - 人間が開発でミスする、ベンダーがワーク・アラウンドを追加する
  - コードのメンテナンスが増加する

- 2019年2月1日:　初めての DNS Flag Day
- 目的:　EDNS ワーク・アラウンドの削除

DNS Flag Day 2019

どのくらいの影響（当時の予想）

2019: T_0 - 3 months, sample 23 M domains

Mode	Permissive (<= 2018)	Strict (2019+)
OK	48.61 %	
Compatible	23.37 %	
High latency	13.15 %	7.48 %
Dead	14.87 %	20.55 %
Breakage		+5.68 %

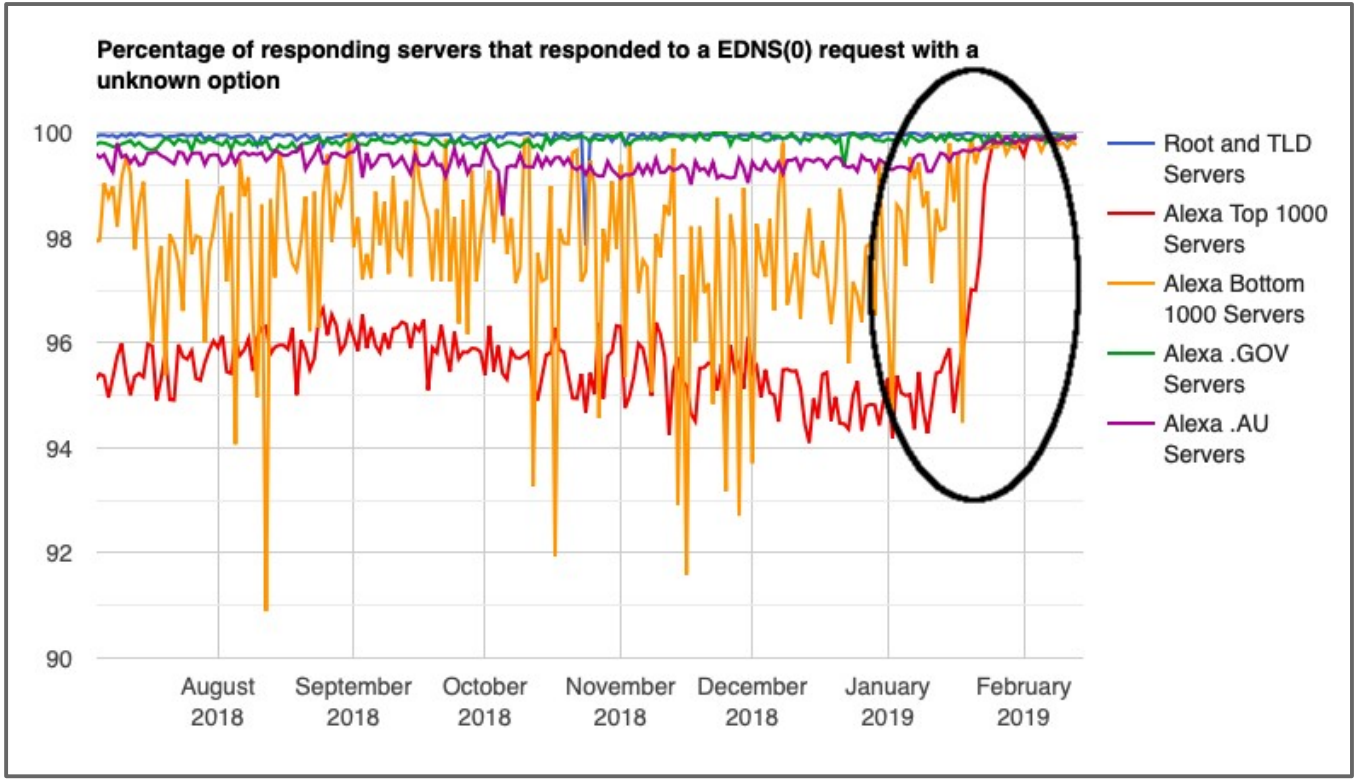
Source: https://ripe78.ripe.net/presentations/53-plenary.pdf

2019: T_0 - 3 months: clusters of breakage

	provider domain	breakage	# broken	
	hichina.com.	35.78 %	469 611	∑
	dnspod.com.	25.66 %	336 797	
	myhostadmin.net.	5.04 %	66 208	66 %
	xincache.com.	4.82 %	63 246	
	dnspod.net.	3.27 %	42 881	
	dnsdun.net.	2.85 %	37 435	
∑	gmoserver.jp.	2.71 %	35 595	
	registrar-servers.com.	1.64 %	21 533	
	alidns.com.	1.63 %	21 369	
85 %	metaregistrar.nl.	1.20 %	15 762	

DNS Flag Day 2019

結果は



Source: https://www.isc.org/blogs/dns-flag-day-was-it-a-success/

DNS Flag Day 2019

協力して、成功でした

Source: https://ripe78.ripe.net/presentations/53-plenary.pdf

DNS Flag Day 2020

それでは、次は？

- 2019-05-12: DNS-OARC30 でパネル・ディスカッション
  - ソフトウェアベンダー： ISC, CZ.NIC, NLnet Labs
  - オペレーター： OpenDNS/Cisco, Quad9, CloudFlare, Google
  - https://youtu.be/mH_elg9EUWw?t=680
  - https://indico.dns-oarc.net/event/31/contributions/678/attachments/673/1102/dns_flag_day_panel.pdf
- 2019-05-21: RIPE78 でアナウンス
  - Petr Špaček (CZ.NIC), Ondřej Surý (ISC)
  - https://ripe78.ripe.net/archives/video/28
  - https://ripe78.ripe.net/presentations/53-plenary.pdf

DNS Flag Day 2020

今回のフォーカス

- 問題:
  - パケット・フラグメンテーション
    - 上手く動作しません
      - https://tools.ietf.org/html/draft-bonica-intarea-frag-fragile
    - セキュアではありません
      - https://tools.ietf.org/html/draft-fujiwara-dnsop-fragment-attack

- ゴール:
  - フラグメンテーションしないように、EDNS Buffer Size を減らしましょう
  - 大きなパケット、UDP から TCP へスイッチしましょう

EDNS Buffer Size

DNS Flag Day 2020

- 詳しい EDNS Buffer Size はまだ決まっていませんが
  - 1220、1232、1280 のいずれになりそう

- 「dig」コマンドでテスト:

```
$ dig +short rs.dns-oarc.net TXT @203.0.113.1
rst.x1188.rs.dns-oarc.net.
rst.x1198.x1188.rs.dns-oarc.net.
rst.x1204.x1198.x1188.rs.dns-oarc.net.
"203.0.113.1 sent EDNS buffer size 1232"
"203.0.113.1 DNS reply size limit is at least 1204"
```

DNS over TCP

DNS Flag Day 2020

- RFC 7766: DNS Transport over TCP – Implementation Requirements
- TCP ポート53で応答
  - DNS サーバーで有効化
  - Firewall をチェック
- なぜ TCP 対応が必要?
  - UDP スプーフィングが簡単
  - Reflection/amplification attacks
  - IP Fragmentation attacks
- なぜ TCP のみではなく?
  - UDP は小さなパケットには問題ない
  - TCP は 4 倍くらい遅い

DNS over TCP

現在の状況

- 調査:
  - 2019年 5 月
  - 3.400 万ドメイン
  - 59 TLDs
- 結果:
  - 7%では TCP の失敗

TCP on auths in May 2019, 34 M domains, 59 TLDs

Mode	TCP as last instance	TCP required
OK	67.52 %	67.52 %
High latency	12.83 %	5.76 %
Dead	19.65 %	26.72 %
Breakage		+7.07 %

email, solutions, tel, date, review, one, link, services, company, agency, group, guru, news, network, photography, studio, jobs, business

net, co, xyz, se, cz, loan, online, club, site, icu, nz, shop, ltd, cl, mobi, app, live, pro, website, space, nu, fun, store, win, tech, men, life, blog, stream, world, dev, wang, bid, rocks, cat, tokyo, xxx, today, design, trade, xin

Source: https://ripe78.ripe.net/presentations/53-plenary.pdf

DNS over TCP

現在の状況

Top ten: TCP-broken providers in May 2019

	provider domain	breakage	# broken
∑	hichina.com	67.84 %	1 610 817
	name-services.com	6.74 %	160 070
	foundationapi.com	3.66 %	86 970
70 %	xincache.com	2.63 %	62 479
	alidns.com	2.16 %	51 309
	123-reg.co.uk	2.04 %	48 411
∑	domainparkingserver.net	1.69 %	40 036
	ztomy.com	1.27 %	30 238
	mytrafficmanagement.com	1.23 %	29 285
90 %	myhostadmin.net	1.05 %	24 856

ソフトウェア･アップデート等が必要？

DNS Flag Day 2020

- サポートされているメージャーのオープンソース DNS ソフトウェアなら
  - アップデートする必要ない

- 但し､場合によって設定変更が必要
  - TCP 対応の有効
  - EDNS Buffer Size の変更
  - Firewall 設定の確認

テスト･ツール

DNS Flag Day 2020

- ウエッブベースのツールは開発中

- 「 dig 」コマンドで、下記のように確認できます

```
$ dig +tcp @auth_IP yourdomain.example.
```

```
$ dig +tcp @resolver_IP yourdomain.example.
```

```
$ dig @resolver_IP test.knot-resolver.cz. TXT
```

詳しくは

ネットにて

- DNS Flag Day ホームページ
  - https://dnsflagday.net/
- アナウンス・メーリングリスト
  - https://lists.dns-oarc.net/mailman/listinfo/dns-announce
- ディスカッション・メーリングリスト
  - https://lists.dns-oarc.net/mailman/listinfo/dns-operations
- Further Issues
  - https://github.com/dns-violations/dnsflagday/issues

ありがとうございます

Stay Open.

連絡しようと思ったら...

Jan HILBERATH （ヤン・ヒルベラート）
<jan.hilberath@open-xchange.com>

OX Dovecot 株式会社
〒 103-0007
東京都中央区日本橋浜町 2-60-10
浜町公園ビル 4F
+81 3 3527 3630

www.open-xchange.com

www.dovecot.co.jp

Stay Open.