フルサービスリゾルバに対する攻撃について

2018年11月29日
Internet Week 2018 DNS DAY

株式会社QTnet
技術本部　サービスオペレーションセンター

末松慶文 (yo_suematsu at qtnet.co.jp)

自己紹介

- 末松慶文(すえまつ よしぶみ)
  - DNSを含むサーバ関連の構築と保守などを10年くらい。
- 株式会社QTnet （旧 九州通信ネットワーク株式会社）
  - 新社名のお知らせ
    https://www.qtnet.co.jp/info/2017/20170614.html
  - QTmobile (QTモバイル)
    https://www.qtmobile.jp
  - DNSの耐障害性強化に向けてJPRSと共同研究を開始 (2015年7月13日)
    JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始　http://jprs.co.jp/press/2015/150713.html
    QTNet: JPRSとの共同研究について　https://www.qtnet.co.jp/info/2016/20160118.html
  - APRICOT 2017 TLD Anycast DNS servers to ISPs (JPRS, QTnet)
    https://2017.apricot.net/program/schedule/#/day/9/network-operations-2
  - JPRSおよび電力系通信事業者8社が共同研究の成果を公開
    https://www.qtnet.co.jp/info/2017/20171031_1.html
    https://tldlabs.jprs/acts/s001/

どのような局面においても名前解決を継続的に提供し続けたい！

フルサービスリゾルバに対する攻撃

- 量による攻撃
  - ・大量のトラフィックを送りつける(DoS, DDoS攻撃)
    -> 2017年の振り返り＆今年は・・・
  - ・水責め攻撃　(フルサービスリゾルバそのものが攻撃対象ではなく、まきぞえ)
    -> 2013年～2018年までの動向

今回はこちらを対象にお話しします。

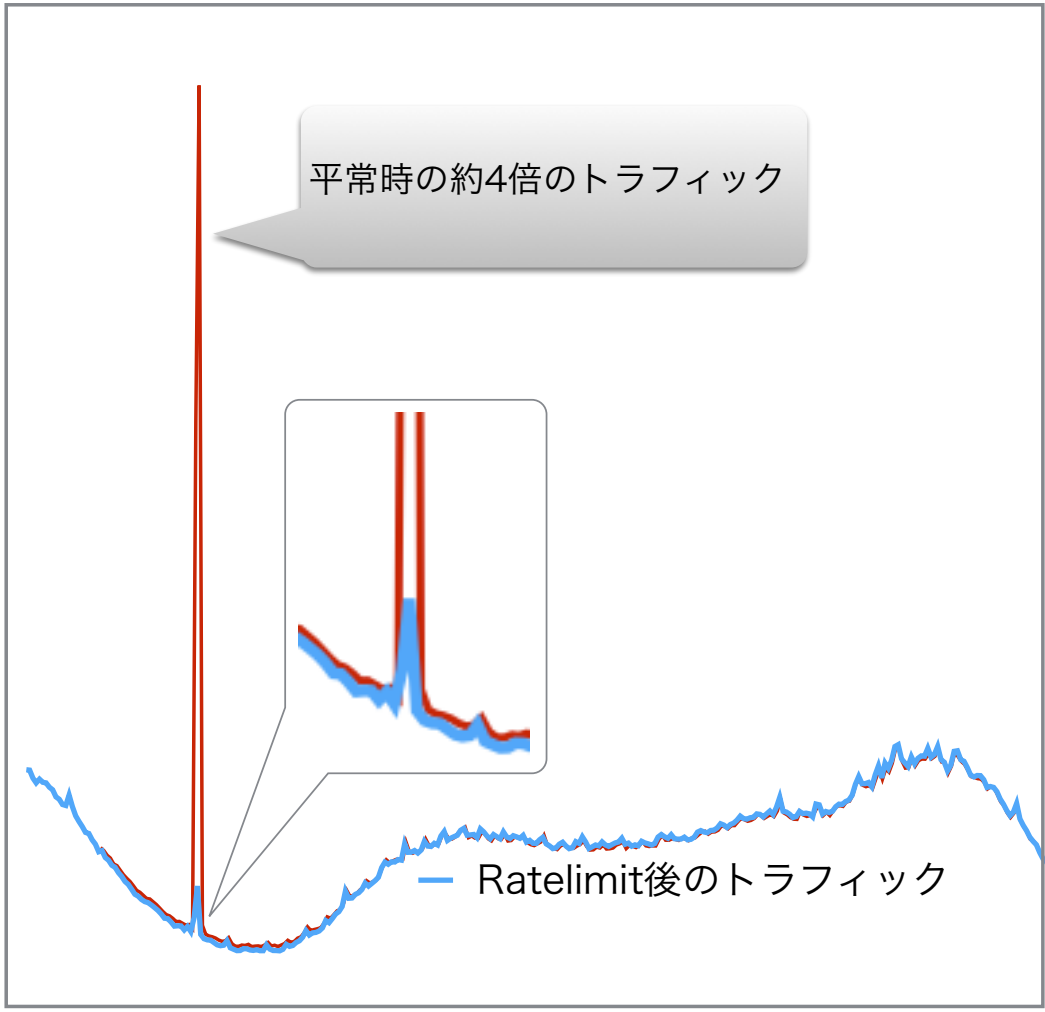
- その他の攻撃
  - ・DNSキャッシュポイズニング攻撃
  - ・DNSアプリケーションの脆弱性に対する攻撃

DoS,DDoS攻撃の発生状況について

DoS, DDoS対策(2017/11/19に発生した攻撃について)

- 攻撃の概要
  - 大量のトラフィックを送りつける攻撃
  - ・国内の複数のISPで攻撃を観測
  - ・一部ISPでは11/18にも発生
  - ・トラフィックの規模はISPにより大幅に異なる
  - ・オープンリゾルバを経由した攻撃ではない？

  - DNS Queryの内容
    - ・ランダムに見える英数字12文字
    - ・query-class (CLASS27764)
    - ・query-type (TYPE30309)



2018年は・・
同様の攻撃は発生せず。その他の大規模な攻撃は発生していない模様

水責め攻撃の状況について

水責め(Water Torture)攻撃とは？

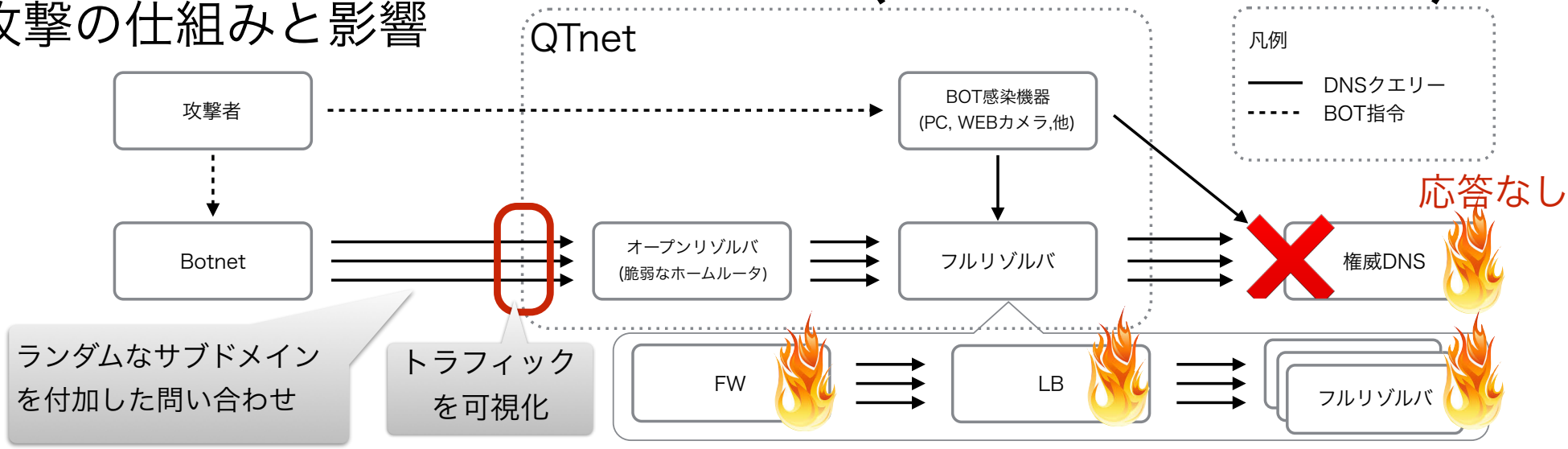
- 水責め攻撃とは？？
  - ・DNSに対するDDoS攻撃の手法の一つ
  - ・2014年初頭より、世界的に観測され始めた。
  - ・真の攻撃対象は権威DNS
    - フルリゾルバも間接的に大きな影響を受ける。
  - ・日本でも影響が観測された。
    - [2014] 6月から7月に日本の多くのISPでも水責めが観測された。
    - [2015] JPドメイン名を標的とした“DNS水責め攻撃”を確認

インターネット定点観測レポート(2015年 1～3月)
<https://www.jpcert.or.jp/tsubame/report/report201501-03.html>

    - [2016] 2016年5月末から9月末まで、攻撃停止
    - [2017] 2017年後半は、水責め攻撃の発生頻度の低下

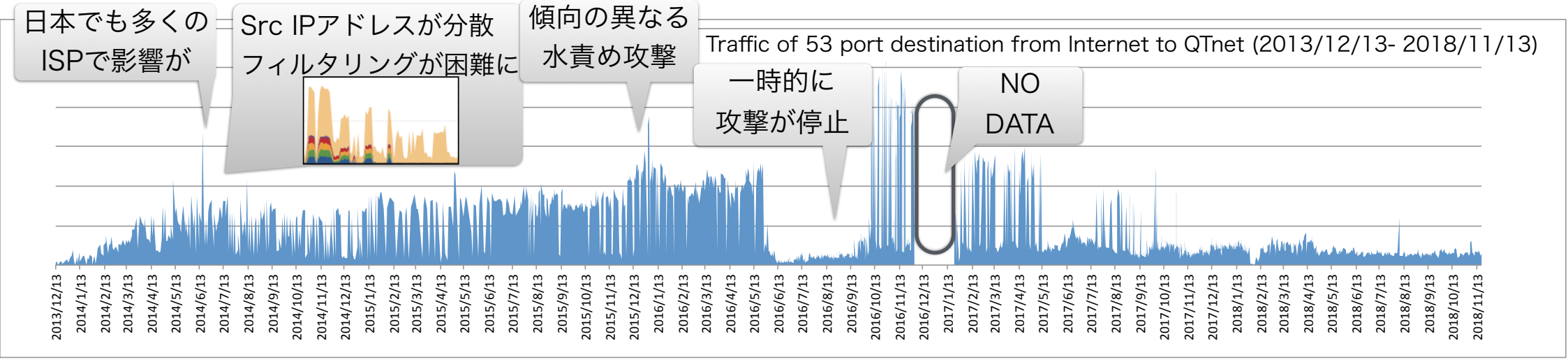
水責め攻撃の動向(2013-2018年)

- 攻撃の仕組みと影響



権威DNSが応答を返せないことで、フルリゾルバ周辺でリソース枯渇に！

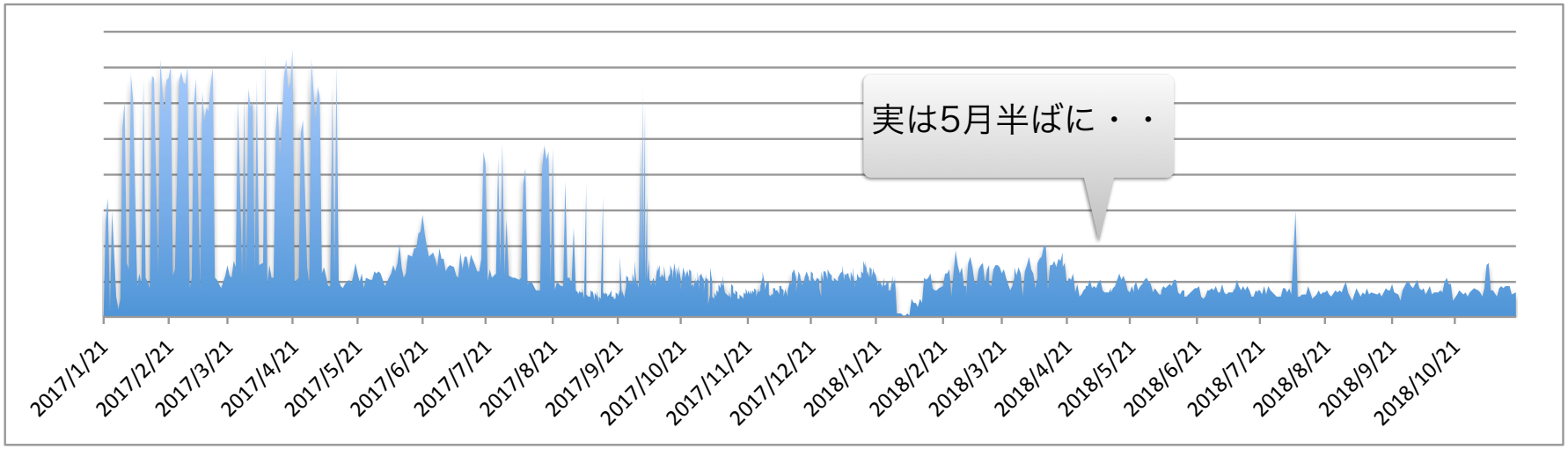
- ISP網内への流入トラフィックの推移



水責め攻撃の動向(2017-2018年)

- ISP網内への流入トラフィックの推移

Traffic of 53 port destination from Internet to QTnet (2013/12/13- 2018/11/13)



- 水責め攻撃への対策手法

・DDoS対策機器、Load Balancer

・BIND 9.11 (fetches-per-zone,fetches-per-server)

Recursive Client Rate limiting - FAQs
https://kb.isc.org/docs/aa-01316

・Unbound 1.7 (aggressive-nsec)

Aggressive use of the DNSSEC-Validated cache in Unbound
https://medium.com/nlnetlabs/aggressive-use-of-the-dnssec-validated-cache-in-unbound-1ab3e315d13f

Aggressive Use of DNSSEC-Validated Cache (RFC8198)
https://tools.ietf.org/html/rfc8198

多くの実装で対策手法も整ってきた。水責め攻撃はほぼ沈静化

権威DNSの障害時に影響を小さくする技術

Serving Stale Data to Improve DNS Resiliency

https://tools.ietf.org/html/draft-ietf-dnsop-serve-stale-02

- BIND 9.12 **New!** 有償版9.11-Sでも使用可、9.12は2019/04にEoL

  - 特徴 (Serve Stale)

    権威DNSから応答がなくても、保持されたキャッシュからクライアントにはTTL=1で応答する。

- Unbound 1.8

  - 特徴 (Serve Expired)

    権威DNSから応答がなくても、保持されたキャッシュからクライアントにはTTL=0で応答する。

https://www.unbound.net/documentation/unbound.conf.html

- Knot Resolver

  - 特徴 (Serve Stale)

    権威DNSの応答がなくてもタイムアウトしたレコードを使用できるようにするdemo module

- Nominum CacheServe

  - 特徴 (Prefetch Extension)

    権威DNSへのprefetchクエリが失敗した場合に、キャッシュの情報を保持。

    prefetchを続けつつ、クライアントにはTTL=0で応答する。

まとめ

- フルサービスリゾルバに対する攻撃について
  - 水責め攻撃の発生状況について
    ・2017年の後半から減少傾向が継続
    ・2018年6月半ばに・・
  - DoS, DDoS攻撃の発生状況について
    ・2017年11月に複数のISPで異常なトラフィックを観測
    ・2018年は、顕著な攻撃は発生していない模様
  - その他
    ・水責め対策が充実してきた
    ・権威DNSの障害時に影響を最小化する技術もでてきた。

通常時からよくデータを観察することで、攻撃の早期発見と攻撃特性から対策を！