Actions against DNS security issues which .JP faced

8th September 2015

APNIC 40 LT Session

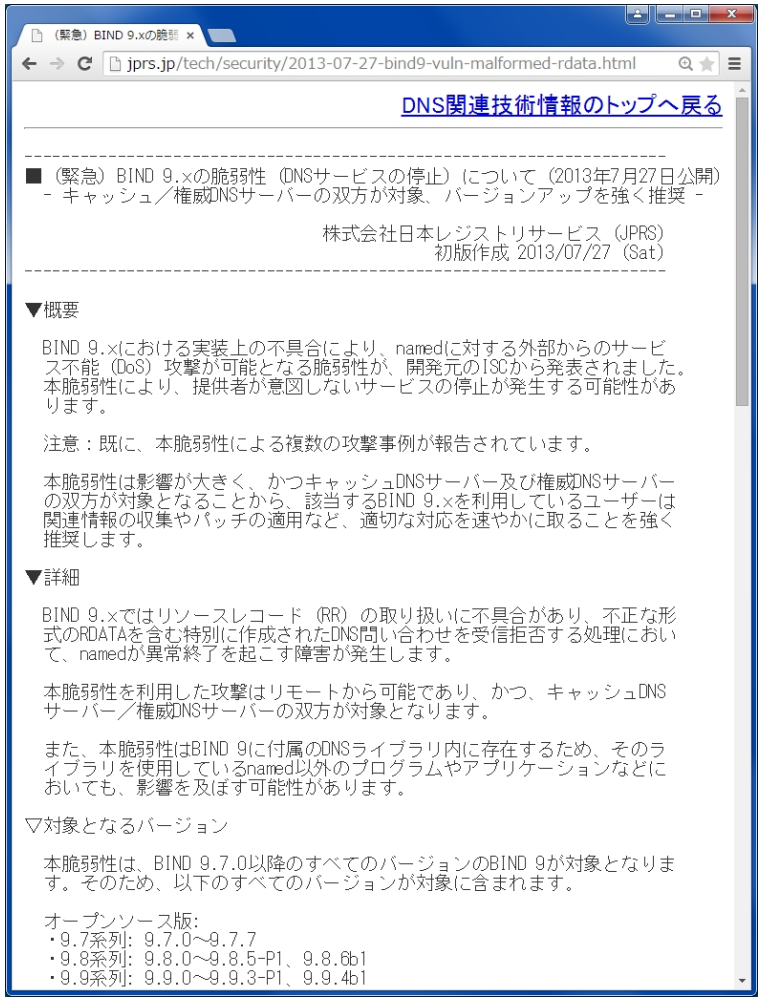
Yoshiro YONEYA <yoshiro.yoneya@jprs.co.jp>

Basic actions

- In general, JPRS (.JP Registry) publishes following documents (in Japanese language) to the public when we faced security issues
  - Security advisory
  - Technical report
- Examples of security issues
  - DNS software vulnerability
  - DNS operational vulnerability
  - Domain name hijacking by unauthorized manipulation of registered data

Example 1: DNS software vulnerability

- Major targets
  - BIND, NSD, Unbound, PowerDNS
- Actions are (almost) routine
  - Prepare security advisory in Japanese language when we receive ASN or security advisory from vendor
  - Publish the advisory synchronized with vendor's disclosure as much as possible
    - JPRS Web, Operator groups' ML, IT media
  - Publish technical report afterwards describing details and countermeasures



（緊急）BIND 9.xの脆弱
jprs.jp/tech/security/2013-07-27-bind9-vuln-malformed-rdata.html

DNS関連技術情報のトップへ戻る

■（緊急）BIND 9.xの脆弱性（DNSサービスの停止）について（2013年7月27日公開）
－ キャッシュ／権威DNSサーバーの双方が対象、バージョンアップを強く推奨 －

株式会社日本レジストリサービス（JPRS）
初版作成 2013/07/27（Sat）

▼概要

BIND 9.xにおける実装上の不具合により、namedに対する外部からのサービス不能（DoS）攻撃が可能となる脆弱性が、開発元のISCから発表されました。本脆弱性により、提供者が意図しないサービスの停止が発生する可能性があります。

注意：既に、本脆弱性による複数の攻撃事例が報告されています。

本脆弱性は影響が大きく、かつキャッシュDNSサーバー及び権威DNSサーバーの双方が対象となることから、該当するBIND 9.xを利用しているユーザーは関連情報の収集やパッチの適用など、適切な対応を速やかに取ることを強く推奨します。

▼詳細

BIND 9.xではリソースレコード（RR）の取り扱いに不具合があり、不正な形式のRDATAを含む特別に作成されたDNS問い合わせを受信拒否する処理において、namedが異常終了を起こす障害が発生します。

本脆弱性を利用した攻撃はリモートから可能であり、かつ、キャッシュDNSサーバー／権威DNSサーバーの双方が対象となります。

また、本脆弱性はBIND 9に付属のDNSライブラリ内に存在するため、そのライブラリを使用しているnamed以外のプログラムやアプリケーションなどにおいても、影響を及ぼす可能性があります。

▽対象となるバージョン

本脆弱性は、BIND 9.7.0以降のすべてのバージョンのBIND 9が対象となります。そのため、以下のすべてのバージョンが対象に含まれます。

オープンソース版:
・9.7系列: 9.7.0～9.7.7
・9.8系列: 9.8.0～9.8.5-P1、9.8.6b1
・9.9系列: 9.9.0～9.9.3-P1、9.9.4b1

Security advisory
(on JPRS Web)

JPRS JAPAN REGISTRY SERVICES
No. 021

JPRS トピックス＆コラム

■Bot経由でDNSサーバーを広く薄く攻撃
～DNS水責め攻撃の概要と対策～

「DNS水責め攻撃」と呼ばれる攻撃手法が、2014年初頭から世界的に観測されています。
今回はこの攻撃手法の概要と、現時点における対策について解説します。

■DNS水責め攻撃の特徴

DNS 水責め攻撃では、攻撃対象のランダムなサブドメインに対する DNS 問い合わせが攻撃に使われます。

asdykuadkncezq.www.example.TLD
ランダムな文字列（サブドメイン）　攻撃対象

図 1：攻撃に使われる問い合わせパターンの例

この問い合わせはカミンスキー型攻撃手法で用いられるものと同一であり、「ランダム DNS クエリー攻撃」や「ランダムサブドメイン攻撃」などとも呼ばれています。

▼攻撃の目的と攻撃対象

DNS 水責め攻撃ではカミンスキー型攻撃手法と異なり、キャッシュポイズニングを目的とした攻撃パケット（偽の DNS 応答）が検出されません。そのため、この攻撃が最初に観測された 2014 年初頭の段階では、攻撃者の真の目的が判然としませんでした。

その後、2014 年 5 月から 7 月にかけ、数多くのドメイン名がこの攻撃の被害を受け、アクセス不能の状態に陥りました。その際の攻撃パターンや攻撃対象の分析結果から、攻撃対象のドメイン名を管理する権威 DNS サーバーに大量の DNS 問い合わせを送り付けることでサービス不能の状態にし、そのドメイン名をアクセス不能の状態に陥らせることが攻撃者の目的であったと考えられています。

▼キャッシュ DNS サーバーにも被害が発生

前述した 2014 年 5 月から 7 月の攻撃では権威 DNS サーバーに加え、日本国内の複数の ISP を含む数多くのキャッシュ DNS サーバーも過負荷の状態となり、一時的にサービス不能の状態に陥りました。

[1] 複数の報告者から、攻撃対象となったドメイン名の多くが中国・台湾・香港の EC サイトやカジノサイトなどであったと報告されています。

■Water Torture = 水責め

2014 年 2 月にこの攻撃について報告した米国 Secure64 Software が、この攻撃手法を「Water Torture（水責め）」と命名しました[2]。同社では命名の由来をかつて中国などで行われていた「Chinese Water Torture[3]（中国式水責め）」であるとしています。

■DNS水責め攻撃の概要

DNS 水責め攻撃では、以下に示す 6 種類の人物が登場します。

図 2：DNS 水責の攻撃の登場人物

▼攻撃者・Botnet

DNS 水責め攻撃を実行する攻撃者は、インターネット上のオープンリゾルバーのリストを持っています。

また、攻撃者は多数の PC などにより構成される Botnet を遠隔操作することで、攻撃を実行します。

▼オープンリゾルバー・欠陥を持つホームルーター

このオープンリゾルバーのリストには DNS サーバーの他、本来受け付けてはならない WAN 側からの問い合わせを受け付けて処理してしまう、欠陥を持つホームルーターも掲載されています。これらは外部から見た場合、いずれもオープンリゾルバーとして動作します。

[2] Water Torture: A Slow Drip DNS DDoS Attack
https://blog.secure64.com/?p=377
[3] Wikipedia Chinese water torture
https://en.wikipedia.org/wiki/Chinese_water_torture

※掲載内容は2015年2月現在のものです。
1

Technical report
(JPRS Topics and Columns)

Example 2: DNS operational vulnerability

- Major targets
  - Attacks to DNS servers
    - Open resolvers (DNS reflection attacks)
    - Non source port randomized (SPR) resolvers (cache poisoning attacks)
- Actions are (basically) routine, but extended case by case
  - Usually, prepare and publish security advisory and technical report in Japanese as well
  - In addition, explanations at public / private fora
    - JANOG meetings, DNS fora, JPRS private seminars
    - Articles to IT/Academic journals

Limitations we found and toward improvement

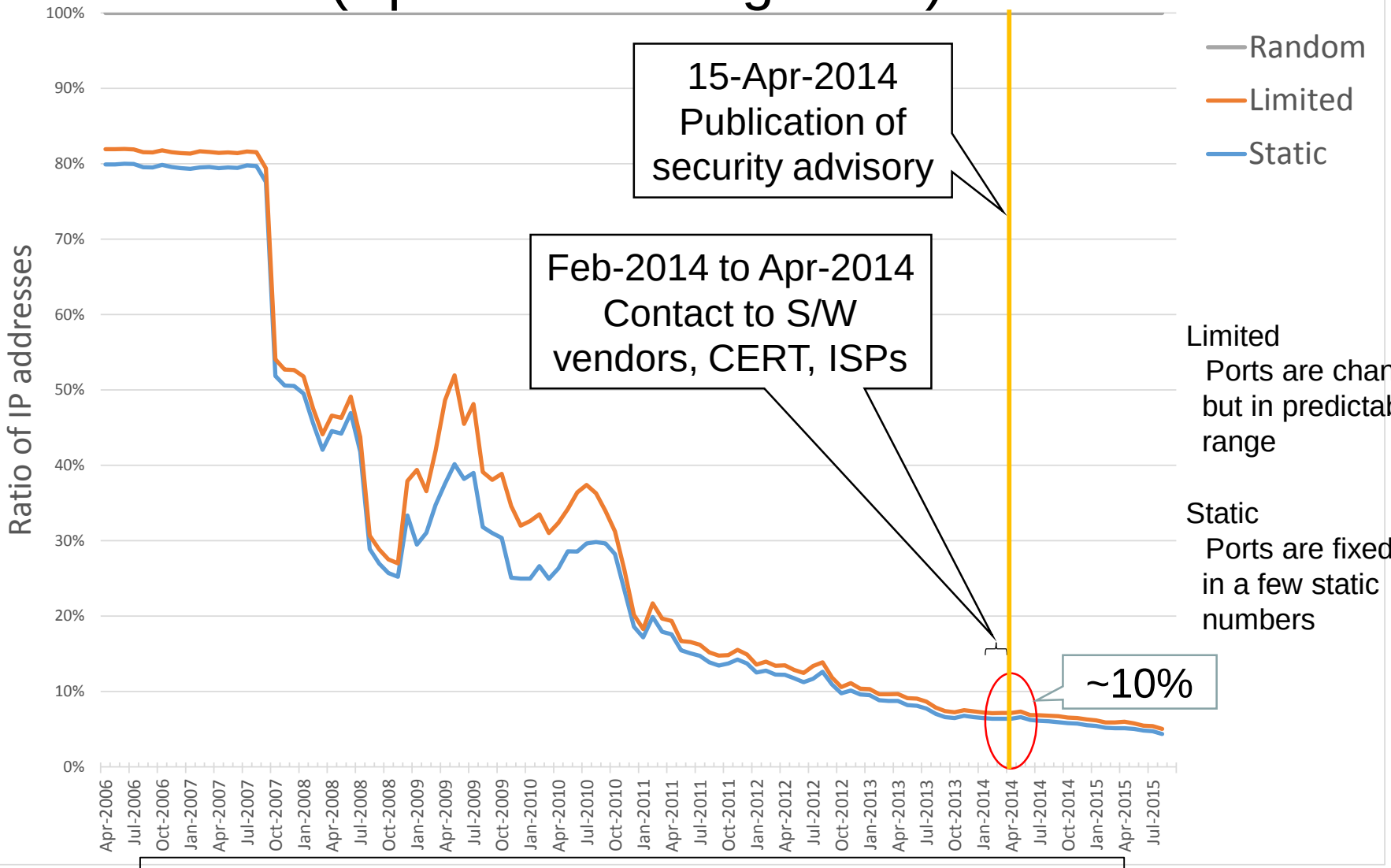
- Public outreach coverage
  - Especially, non-IT media, H/W vendors, enterprises, end users
- Accumulation and sharing of best practices
  - Especially, how ISPs and registrars approach and persuade customers

… so we started individual negotiation and collaboration with relevant organizations

Example of individual negotiation and collaboration (1/2)

- Cache poisoning attacks regarding node re-delegation (2014)
  - Poison injection to “empty non-terminals”
  - .JP structure has many “empty non-terminals”
  - Details can be found at <http://www.iepg.org/2014-07-20-ietf90/201407-poisoning.pdf>
  - Non negligible number (~10%) of resolvers may be affected (#8)

Transition of source port randomization status (Apr-2006 to Aug-2015)



Limited
Ports are changed but in predictable range

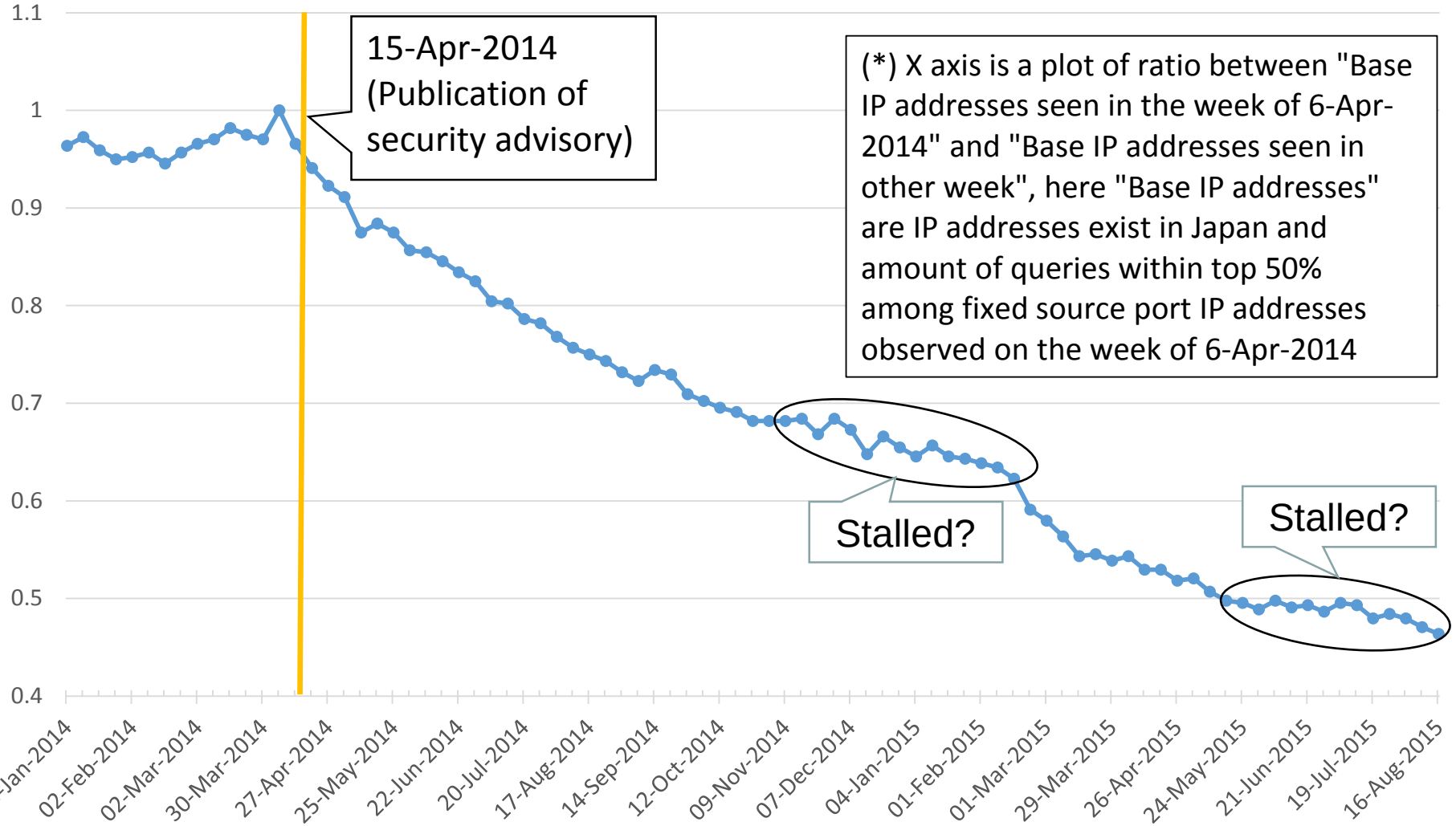
Static
Ports are fixed in a few static numbers

Observed by JPRS. Source port numbers by each IP address that sends more than 10 queries per day from query log of some JP DNS servers.

Example of individual negotiation and collaboration (2/2)

- Actions we took / are still taking
  - Contact DNS software vendors for asking about effective countermeasures
  - Contact domestic CERT organizations for information sharing and deciding each other's actions
  - Contact major domestic ISPs for information sharing and soliciting direct alert to their customers
  - Provide vulnerable resolvers' information to our registrars periodically (per month) and soliciting direct alert as well
  - Interview to several registrars for their successful practices
    - Observed stalemate situation in some registrars (#10)

Situation of decrease of fixed source port IP addresses(*) (as of 17-Aug-2015)



For better public outreach

- Establishing confidential communication path for DNS security issues with domestic CERT organizations
  - For generalization of node re-delegation case
  - For wider outreach to media, vendors and end users
    - Unification of terminology and mutual reference of explanations for helping understanding of multi-level readers
  - And this formation is now utilizing for sharing information such as random subdomain attacks and domain name hijacking cases
- Accumulating best practices
  - For encouraging passive ISPs/registrars
  - For improving effect of direct alerts

Ongoing Work

- Our actions are still underway, and need further improvement
  - To overcome difficulties of the last reach
  - To have rational balancing point between cost and effect