2015年のroutesec動向

Internet Multifeed / JPNAP
Tomoya Yoshida
<yoshida@mfeed.ad.jp>

内容

- 最近流行しているハイジャック事例
- 肥大化する経路情報と注意喚起
- うるう秒2015
- その他国際動向

内容

- 最近流行しているハイジャック
- 肥大化する経路情報と注意喚起
- うるう秒2015
- その他国際動向

最近流行しているハイジャック

- 局所的なハイジャック
  - グローバルインターネット全体へ経路広報するのではなく、BGPのno-export community等を付与するなどして、一部の（狙い撃ちの）ピア先にのみ不正な経路を流し、必要な情報を盗み見る、など
    - 例）ビットコインのやり取りを盗む
  - Longer-prefixを再広告することで奪回可能だが、そもそも検出が難しいという問題がある

- 未利用アドレスのハイジャック
  - 後述

JPIRRによるハイジャック検出

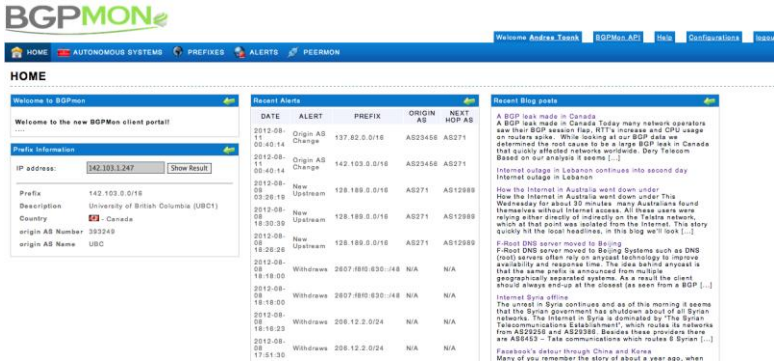
route: 202.12.30.0/24
descr: JPNICNET
Japan Network Information Center
Kokusai Kogyo Kanda Bldg. 6F
2-3-4 Uchi-Kanda
Chiyoda-ku, Tokyo 101-0047
JAPAN
X-Keiro: okadams@nic.ad.jp
X-Keiro: okadams-noc@nic.ad.jp
origin: AS2515
admin-c: SN3603JP
tech-c: YK11438JP
tech-c: MO5920JP
notify: system@nic.ad.jp
mnt-by: MAINT-AS2515
changed: apnic-ftp@nic.ad.jp 20080116
source: JPIRR

登録されたorigin情報とは異なるoriginASから経路広報が(経路奉行で)検出された場合に、「X-Keiro:」に記載のあて先にメール通知する

<--追加記述
<--複数あて先に通知する場合記述

世界の主な経路検出システム

- BGPmon
  - 5経路まで無料
  - それ以上は1経路あたり月13$
- JPIRR
- Dyn(renesys)
- thousandeyes



未利用アドレスのハイジャック

- インターネット上に広告されていないIP Prefixが勝手に経路広告されて、SPAM配信等に利用される被害が増大
  - 内部でグローバルアドレスを利用しているケース
  - 保有はしているけど実際には未使用 or 利用開始前

- 2015年の被害例
  - 複数のNTT-NGNアドレスが勝手に使われていた。。
    - ブルガリアや中国から別ドメインと組み合わせて利用
    - RIPE DBにも登録情報があり、追跡するとかなり怪しい。
  - IIJで、アドレス移転に伴い取得したIPアドレスが、利用前に勝手に使われていた（janogレポート@松崎さん)。。
    - 証明書まで偽造されていて、こちらも怪しい。
  - そのIIJのアドレスの真後ろのIPを保有している人も、類似被害にあっていた。。
  - その他にも沢山の報告があがっている

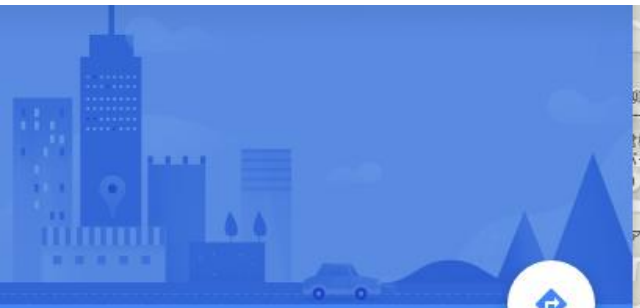
NTT-NGNの被害例

route: 124.245.0.0/16
descr: nipponroute
origin: AS7688
mnt-by: nipponmish-mnt
mnt-by: RIPE-NCC-RPSL-MNT
created: 2013-12-18T19:33:12Z
last-modified: 2013-12-18T19:33:12Z
source: RIPE # Filtered

mntner: nipponmish-mnt
descr: Maintainer
admin-c: HZ1260-RIPE
upd-to: hui.zao@nippontelecom.com
auth: MD5-PW # Filtered
mnt-by: nipponmish-mnt
notify: hui.zao@nippontelecom.com
changed: hui.zao@nippontelecom.com 20131218
remarks: Accepted the RIPE Database Terms and Conditions
created: 2013-12-18T19:19:48Z
last-modified: 2013-12-18T19:19:48Z
source: RIPE # Filtered

person: Hui Zao
address: 3-9-11 Midori-cho, Musashino-shi
phone: +81-422-59-7351
e-mail: hui.zao@nippontelecom.com
nic-hdl: HZ1260-RIPE
mnt-by: nipponmish-mnt
changed: hui.zao@nippontelecom.com 20131218
created: 2013-12-18T19:19:48Z
last-modified: 2013-12-18T19:19:48Z
source: RIPE

怪しい情報が何故か
RIPE DBに登録されていた。。



〒180-0012 東京都武蔵野市緑町３丁目９−１１

ルート・乗換

保存　付近を検索　共有

地図に載っていない場所を追加

よしださん，

研究所の社内名簿検索しましたが，やはり Zao さんは
いないですね．

ＮＴＴ ＮＴ研　　藤崎 智宏 (Ｃｏ Ｃｏ じゃなくてもはねだ・えりか)
Tel: 04xx-xx-xxxx Fax: 04xx-xx-xxxx

RIPE-NCC-RPSL-MNTの存在

You will be able to delete the object by using then public password of the mntner RIPE-NCC-RPSL-MNT.

This maintainer is used to let people add a route object which address space and/or AS number are outside the RIPE region.

The password is mentioned in the remarks of the object itself:
mntner: RIPE-NCC-RPSL-MNT
descr: This maintainer may be used to create objects to represent
descr: routing policy in the RIPE Database for number resources not
descr: allocated or assigned from the RIPE NCC.
admin-c: RD132-RIPE
auth: MD5-PW # Filtered
remarks: **********
remarks: * The password for this object is 'RPSL', without the *
remarks: * quotes. Do NOT use this maintainer as 'mnt-by'. *
remarks: **********
mnt-by: RIPE-DBM-MNT
referral-by: RIPE-DBM-MNT
source: RIPE # Filtered

実は、自由度の高い「RIPE-NCC-RPSL-MNT」というメンテナーが存在し、それを利用して登録されていた。。

ということで、JPNICで簡単に削除できました

Ref: SBL265093

124.245.0.0/16 is listed on the Spamhaus Block List - SBL

124.245.0.0/16 is listed on the Don't Route or Peer List - DROP

2015-09-19 13:17:28 GMT | ntt.net

NIPPON TELEGRAPH AND TELEFHONE WEST CORPORATION (AS1273)

Based on research, analysis of network records, our own intelligence sources and our experience, Spamhaus believes that this IP address range is being used or is about to be used for the purpose of high volume spam emission.

As a precaution we are listing this range in an SBL Advisory until we are able to determine with certainty exactly who is operating these domains/hosts/servers and also verify the opt-in permission status and origin of whatever lists are used for those mailings.

Network Information:
[Network Number] 124.245.0.0/16
[Network Name]
[Organization] NIPPON TELEGRAPH AND TELEFHONE WEST CORPORATION
[Administrative Contact] KU1605JP
[Technical Contact] KU1605JP
[Abuse] jpnic-tec@ml.hq.west.ntt.co.jp
[Allocated Date] 2007/10/04
[Last Update] 2007/10/04 18:51:38(JST)

Domain Name: nunnativ.net
Registry Domain ID: D400353347
Registrar WHOIS Server: Whois.domainerschoice.com
Updated date: 2015-04-06T03:13:09Z
Creation date: 2015-03-28T06:10:14Z

2015/9/7 janogML by peter@ixp.jp

JPNIC? http://www.spamhaus.org/sbl/query/SBL268451
RICOH http://www.spamhaus.org/sbl/query/SBL268217
KAWASAKI HEAVY INDUSTRIES http://www.spamhaus.org/sbl/query/SBL268212
TOKYO KOUGAKUIN http://www.spamhaus.org/sbl/query/SBL268203

NIDEC SANYO http://www.spamhaus.org/sbl/query/SBL267366
NTT WEST http://www.spamhaus.org/sbl/query/SBL265093
NTT EAST http://www.spamhaus.org/sbl/query/SBL262422
CAC (zombie?) http://www.spamhaus.org/sbl/query/SBL253946

TOKYU CONSTRUCTION http://www.spamhaus.org/sbl/query/SBL249300
MURATA http://www.spamhaus.org/sbl/query/SBL247800 (those dancing robots are so cute!)
LEILIAN http://www.spamhaus.org/sbl/query/SBL247797
FUJITSU http://www.spamhaus.org/sbl/query/SBL233285

KYOWA HAKKO http://www.spamhaus.org/sbl/query/SBL229889
TOYOTECH http://www.spamhaus.org/sbl/query/SBL222568
CORPOVEN (dead company?) http://www.spamhaus.org/sbl/query/SBL222563

dig X.X.X.X.zen.spamhous.org

$ dig 0.0.245.124.zen.spamhaus.org

```
; <<>> DiG 9.8.3-P1 <<>> 0.0.245.124.zen.spamhaus.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42660
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 21, ADDITIONAL: 4

;; QUESTION SECTION:
;0.0.245.124.zen.spamhaus.org.          IN          A

;; ANSWER SECTION:
0.0.245.124.zen.spamhaus.org. 60 IN   A          127.0.0.2
```

ZEN Return Codes

Querying zen.spamhaus.org returns the following result codes for listed entries (see the FAQs for a more complete return code table):

Return Codes	Data Source	Contains
127.0.0.2	SBL Advisory	Direct UBE sources, spam operations & spam services
127.0.0.3	CSS SBL ADVISORY COMPONENT	Direct snowshoe spam sources detected via automation
127.0.0.4-7	XBL Advisory	CBL (3rd party exploits such as proxies, trojans, etc.)
127.0.0.10-11	PBL Advisory	End-user Non-MTA IP addresses set by ISP outbound mail policy

http://www.spamhaus.org/zen/

JPNAPセグメントのハイジャック

2014年2月、 弊社JPNAPののセグメント(/24)で“経路ハイジャックを使ったSPAM”を、ロ●アのASにやられました

時系列(JST)

2/11 23:47 経路奉行で経路ハイジャック発生検知
(218.100.45.0/24)

2/12 13:22 SPAM送信
(218.100.45.34, JPNAP未割当IP)

2/12 13:27 spamcopがSPAM検出

2/12 14:40 経路奉行で経路ハイジャック回復検知

2/12 PM spamcopからのメールに気づき対応
=> SPAMメールヘッダのMXレコードはすでに存在せず。

未利用IPを勝手に使う
組織的な犯罪との見方が強い

spamcopからのアラートメール

[SpamCop (218.100.45.34) id:6074690948]A sweet deal! Moto X. No contract. No down payment..

[SpamCop V4.8.1.007]

This message is brief for your comfort. Please use links below for details.

Email from 218.100.45.34 / Tue, 11 Feb 2014 22:27:49 -0600

http://www.spamcop.net/w3m?i=z6074690948z4d537a65b10c84041666fb2664f998cez

[Offending message]

Return-path: <Motorola@wappextil.com>

Received: from wappextil.com ([unknown] [218.100.45.34])
by vms172083.mailsrvcs.net
(Sun Java(tm) System Messaging Server 7u2-7.02 32bit (built Apr 16 2009))
with ESMTP id <0N0V004K08E3TI20@vms172083.mailsrvcs.net> for
x; Tue, 11 Feb 2014 22:27:49 -0600 (CST)

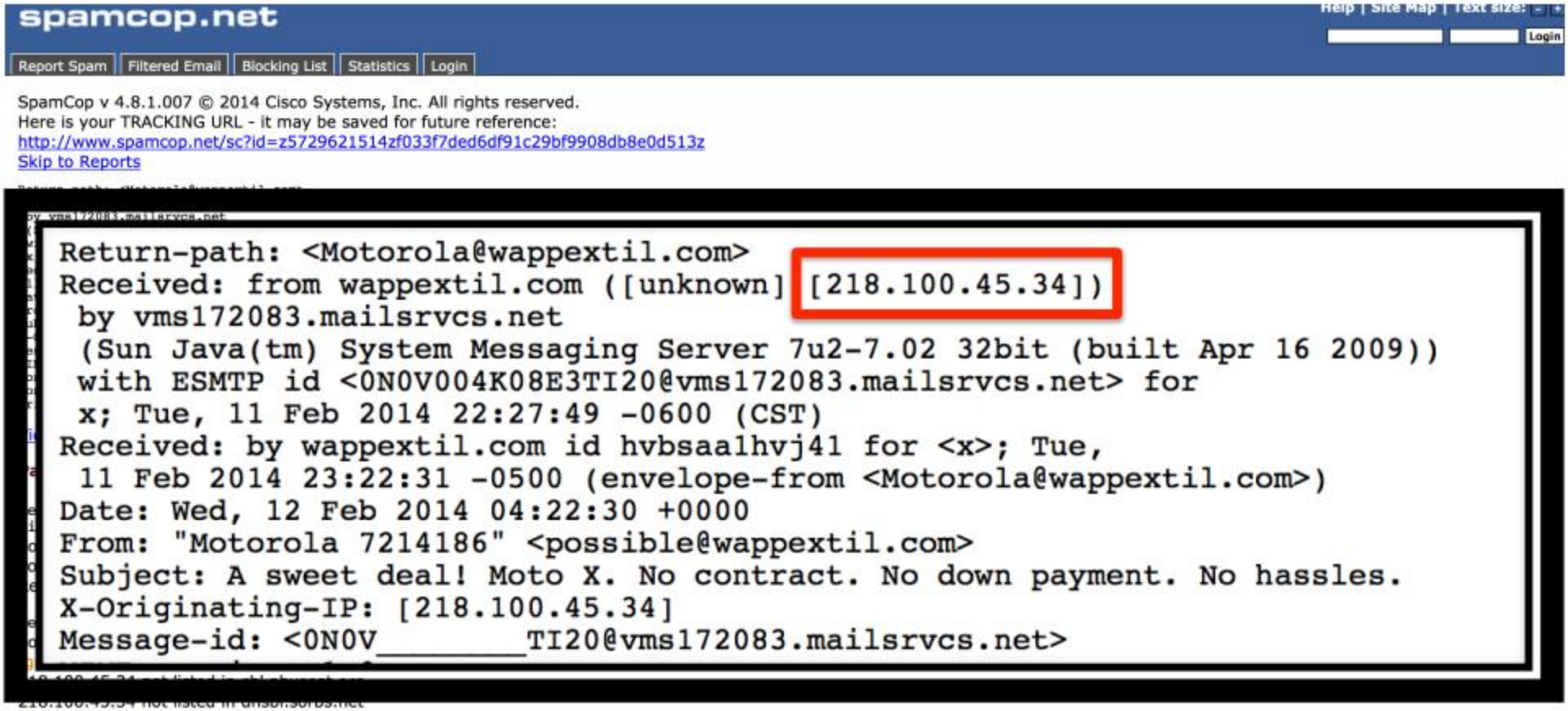
Received: by wappextil.com id hvbsaa1hvj41 for <x>; Tue,
11 Feb 2014 23:22:31 -0500 (envelope-from <Motorola@wappextil.com>)

Date: Wed, 12 Feb 2014 04:22:30 +0000

From: "Motorola 7214186" <possible@wappextil.com>

Subject: A sweet deal! Moto X. No contract. No down payment. No hassles.

-- 以下、spamメールの内容添付 --


spamcop.net
Help | Site Map | Text size:
Login
Report Spam
Filtered Email
Blocking List
Statistics
Login
SpamCop v 4.8.1.007 © 2014 Cisco Systems, Inc. All rights reserved.
Here is your TRACKING URL - it may be saved for future reference:
http://www.spamcop.net/sc?id=z5729621514zf033f7ded6df91c29bf9908db8e0d513z
Skip to Reports
Return-path: <Motorola@wappextil.com>
Received: from wappextil.com ([unknown] [218.100.45.34])
by vms172083.mailsrvcs.net
(Sun Java(tm) System Messaging Server 7u2-7.02 32bit (built Apr 16 2009))
with ESMTP id <0N0V004K08E3TI20@vms172083.mailsrvcs.net> for
x; Tue, 11 Feb 2014 22:27:49 -0600 (CST)
Received: by wappextil.com id hvbsaalhvj41 for <x>; Tue,
11 Feb 2014 23:22:31 -0500 (envelope-from <Motorola@wappextil.com>)
Date: Wed, 12 Feb 2014 04:22:30 +0000
From: "Motorola 7214186" <possible@wappextil.com>
Subject: A sweet deal! Moto X. No contract. No down payment. No hassles.
X-Originating-IP: [218.100.45.34]
Message-id: <0N0V_____TI20@vms172083.mailsrvcs.net>
218.100.45.34 is not an MX for vms172083.mailsrvcs.net
218.100.45.34 is not an MX for vms172083.mailsrvcs.net
Tracking message source: 218.100.45.34:
Routing details for 218.100.45.34
[refresh/show] Cached whois for 218.100.45.34 : tech-c@mfeed.ad.jp
Using last resort contacts tech-c@mfeed.ad.jp
Sorry, this email is too old to file a spam report. You must report spam within 2 days of receipt. This mail was received on Tue, 11 Feb 2014 22:27:49 -0600

	2/10			2/11						2/12			
	15:00	19:00	23:00	3:00	7:00	11:00	15:00	19:00	23:00	3:00	7:00	11:00	15:00
1.2.8.0/22													
163.227.225.0/24													
176.125.32.0/19													
185.6.224.0/22													
185.35.244.0/24													
185.36.68.0/22													
185.36.228.0/22													
196.2.4.0/22													
218.100.2.0/24													
218.100.13.0/24													
218.100.23.0/24													
103.25.220.0/24													
160.20.240.0/24													
185.16.192.0/22													
185.22.172.0/22													
185.33.28.0/22													
185.33.72.0/22													
185.36.248.0/22													
218.100.5.0/24													
218.100.30.0/24													
218.100.45.0/24								JPNAP Tokyo II					
36.37.39.0/24													
91.193.152.0/22													
91.210.64.0/22													
103.11.21.0/24													
103.243.17.0/24													
163.227.124.0/24													
185.20.56.0/22													
185.28.80.0/22													
185.31.224.0/22													
218.100.27.0/24													

Prefix	Desc
218.100.2.0/24	Sydney IX Lan
218.100.5.0/24	OBIS-IX,Internet Exchange Point,Okayama,Japan
218.100.13.0/24	Melbourne IX Lan
218.100.23.0/24	Dunedin Peering Exchange
218.100.27.0/24	OpenIXP, Internet Exchange Point, Indonesia
218.100.30.0/24	APJII Indonesia Internet eXchange
218.100.45.0/24	JPNAP Tokyo II IX

とりうる対策

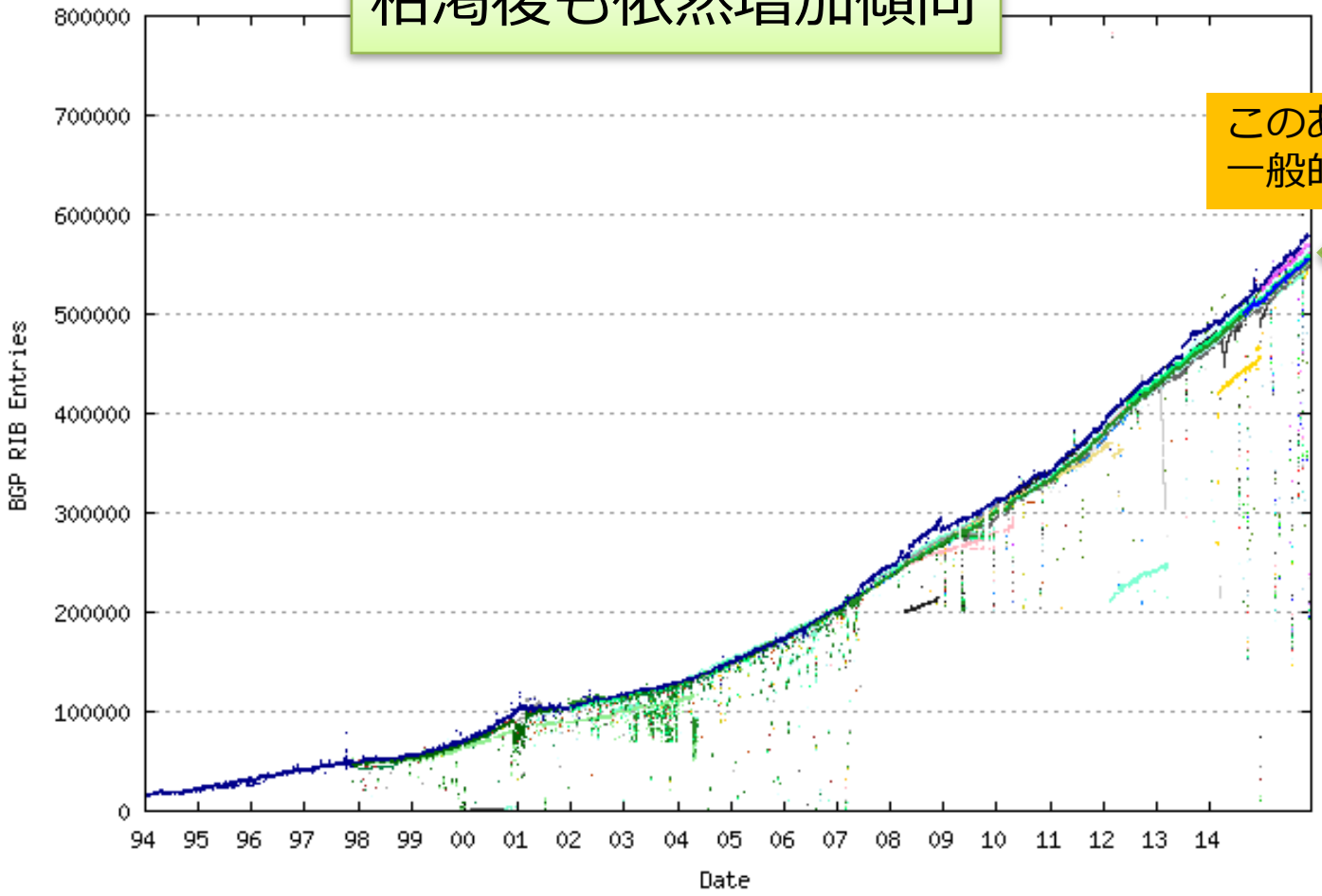
- 利用状態にする（経路を流しておく）
  - 未広告アドレス空間を狙った攻撃には恐らく効果があると想定される
    - 加害者の意図としては、なるべくばれないようにやっているので。。
  - 本来流すべきではないPrefixを経路広告する方法自体は本流の対処ではないけど、背に腹は代えられないかも。。

内容

- 最近流行しているハイジャック事例
- 肥大化する経路情報と注意喚起
- うるう秒2015
- その他国際動向

IPv4経路数の推移

枯渇後も依然増加傾向



このあたりが
一般的な経路数

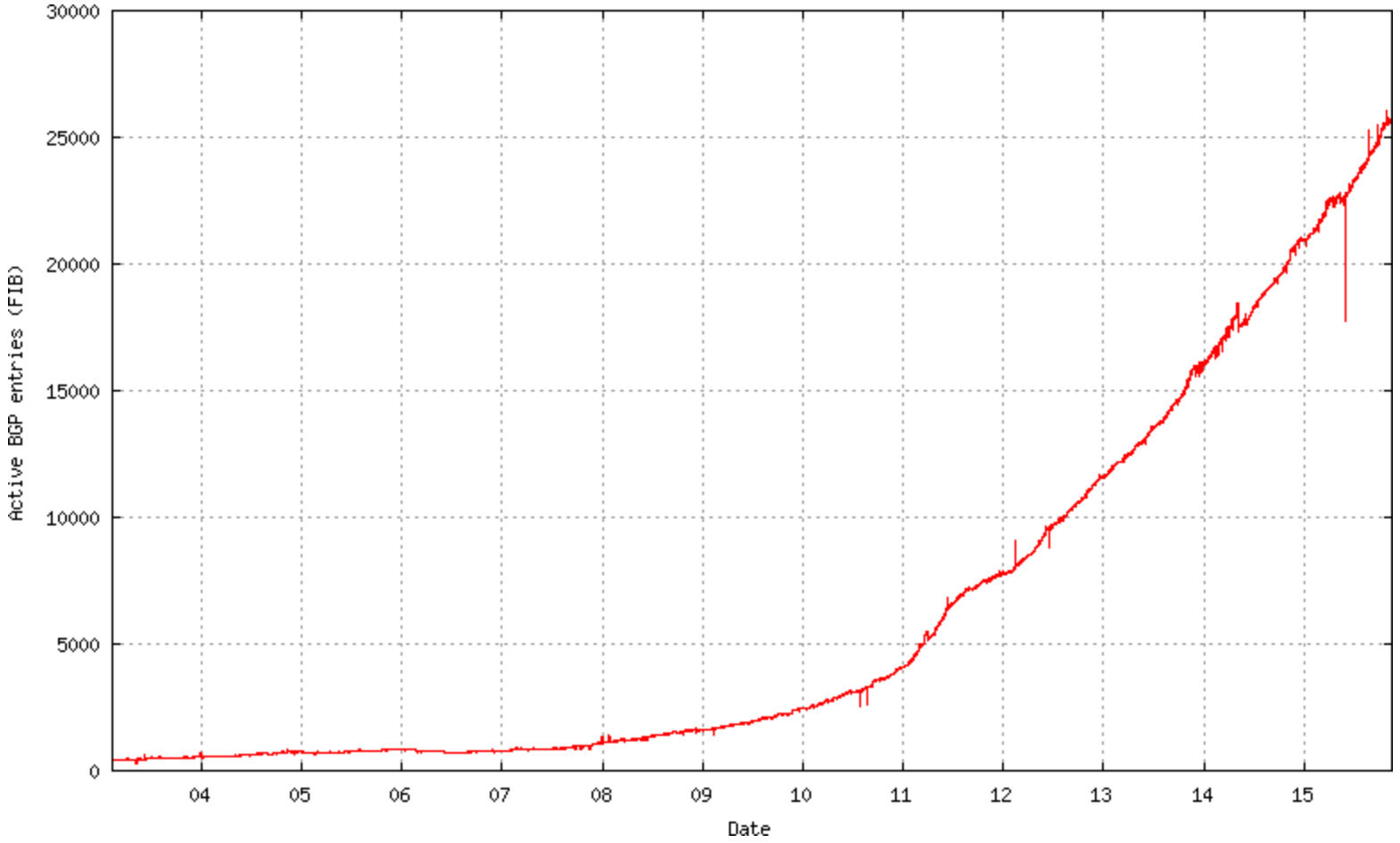
http://bgp.potaroo.net/

IPv4フルルート512Kの壁(2014年)

- JANOG等でも注意喚起がされていた
- が、ばたばた512Kの壁にやられた人が散見
  - JPNAPでも複数の緊急メンテナンスを実施されているISPさんがいた
  - 192K, 224K等昔の頃よりは少なかった？
  - 内部BGP経路が大量に存在するISPでは600K前後

- フルルートが悪だといった風潮は間違い
- 適切にフルルートを活用し、インターネットのルーティングを行う必要がある

最近のIPv6経路増も要注意



異常状態（例えば、細かい経路が急増したとか）への対処も重要

Brocade製品例（参考）

CAMプロファイル
–Xモジュール

X2モジュールではIPv6共に64K

Profile	IPv4	ipv6	MAC/ VPLS MAC	IPv4 VPN	Ipv4/L2 Inbound ACL	IPv6 Inbound ACL	Ipv4/L2 Outbound ACL	IPv6 Outbound ACL
Default Profile	512K	64K	128K	128K	48K	4K	48K	4K
IPv4 Profile	1M	0	32K	0	112K	0	64K	0
IPv6 Profile	64K	240K	32K	0	16K	24K	16K	12K
l2-metro Profile	256K	0	512K	0	64K	0	64K	0
mpls-l3vpn Profile	256K	0	32K	480K	64K	0	64K	0
mpls-vpls Profile	256K	0	512K	0	64K	0	64K	0
multi-service Profile	256K	32K	192K	256K	32K	8K	32K	8K
multi-service-2 Profile	384K	96K	128K	128K	48K	4K	48K	4K
mpls-vpn-vpls Profile	128K	0	224K	384K	48K	0	64K	0
ipv4-vpn Profile	320K	0	32K	448K	64K	0	64K	0
l2- metro-2 Profile	64K	0	608K	0	64K	0	64K	0
mpls-l3vpn-2 Profile	128K	0	32K	544K	64K	0	64K	0
mpls-vpls-2 Profile	128K	0	576K	0	64K	0	64K	0
ipv4-ipv6 Profile	320K	160K	32K	0	48K	20K	32K	8K
ipv4-ipv6-2 Profile	768K	64K	64K	0	64K	8K	48K	4K
ipv4-vpls Profile	320K	0	480K	0	64K	0	64K	0

ipv4-ipv6-2 Profile なら対処可。ただしIPv6の64Kの壁あり

Brocade製品例（参考）

CERシリーズは最大IPv4 150万経路までサポート可能

Feature	NetIron CES	NetIron CER	NetIron CER – RT	MLXe
IPv4 RIB	256K	10M	10M	10M
IPv4 FIB	32K	512K	**1.5M**	1M
IPv6 FIB	8K	128K	**256K**	240K
BGPピア	64	256	256	2000
VRF	16	128	128	2K
VLL	512	1536	1536	48K
VPLS	128	1K	1K	16K

Alaxala製品例（参考）

- AX8600R
  - Defaultの設定で対応済み

表3-8　router-1の経路系テーブルエントリ数(1/2)

パターン名	IPv4ユニキャスト経路	IPv4マルチキャスト経路	IPv6ユニキャスト経路	IPv6マルチキャスト経路
default	1015808	8000	425984	8000
ipv4-uni	1998848	0	0	0
ipv6-uni	32768	0	983040	0
ipv4-ipv6-uni	884736	0	557056	0

http://www.alaxala.com/jp/techinfo/archive/manual/AX8600R/HTML/12_4/CFGUIDE/0019.HTM#ID00066

- AX7800R, AX7700R
  - router-b2で対応は可（ただしIPv4に特化）

表3-12　PRU-B2，PRU-B2B，PRU-C2，PRU-D2およびPRU-D2Bのテーブルエントリの配分パターン

想定する利用形態		パターン名			
		router-b1	router-b2	router-b3	vpnrouter-d1
		ルータ IPv4を主に使用	ルータ IPv4特化	ルータ IPv6を主に使用	ルータ MPLSを使用
IPv4	ユニキャスト経路※	393,216 (384k)	1,048,576 (1024k)	262,144 (256k)	131,072 (128k)
	VPNユニキャスト経路※	－	－	－	262,144 (256k)
	マルチキャスト経路	8,192 (8k)	－	8,192 (8k)	－
	ARP	131,072 (128k)	131,072 (128k)	65,536 (64k)	32,768 (32k)
IPv6	ユニキャスト経路※	65,536 (64k)	－	131,072 (128k)	65,536 (64k)
	VPNユニキャスト経路※	－	－	－	－
	マルチキャスト経路	8,192 (8k)	－	8,192 (8k)	－
	NDP	32,768 (32k)	－	32,768 (32k)	32,768 (32k)

http://www.alaxala.com/jp/techinfo/archive/manual/AX7800R/HTML/10_10_/APGUIDE/0031.HTM

日立製品例（参考）

- GR4000
  - router-b2で対応は可（ただしIPv4に特化）

表 3-7　PRU-B，PRU-B2，PRU-B2B，PRU-C2，PRU-D2 および PRU-D2B のテーブルエントリの配分パターン

想定する利用形態		パターン名			
		router-b1	router-b2	router-b3	vpnrouter-d1
		ルータ IPv4 を主に使用	ルータ IPv4 特化	ルータ IPv6 を主に使用	ルータ MPLS を使用
IPv4	ユニキャスト 経路※	393,216 (384k)	1,048,576 (1024k)	262,144 (256k)	131,072 (128k)
	VPN ユニキャスト 経路※	−	−	−	262,144 (256k)
	マルチキャスト 経路	8,192 (8k)	−	8,192 (8k)	−
	ARP	131,072 (128k)	131,072 (128k)	65,536 (64k)	32,768 (32k)
IPv6	ユニキャスト 経路※	65,536 (64k)	−	131,072 (128k)	65,536 (64k)

http://www.hitachi.co.jp/Prod/comp/network/manual/router/gr4k/1010r1/PDF/APGUIDE/APGUIDE.PDF

他（参考）

- Cisco
  - http://blogs.cisco.com/sp/global-internet-routing-table-reaches-512k-milestone/
- Juniper
  - Routing Engine: RE-850-1536-S
  - CFEB: FEB-M10i-M7i-S
    - RIB IPv4 capacity = 6M
    - FIB IPv4 capacity = 550K
    - RIB IPv6: 3M
    - FIB IPv6: 375K

今後の見通しと対応策

- 当面(2-3年)は現在の傾向に沿って増加し続けると推察
- 対応策
  - 機器等の更改
  - フルルートが不要なドメインは経路削減を実施
    - ルーティングループが発生しないように注意が必要
- 利用しているルータ機器等の特性を把握しておく
- コミュニティの情報をきちんと得る

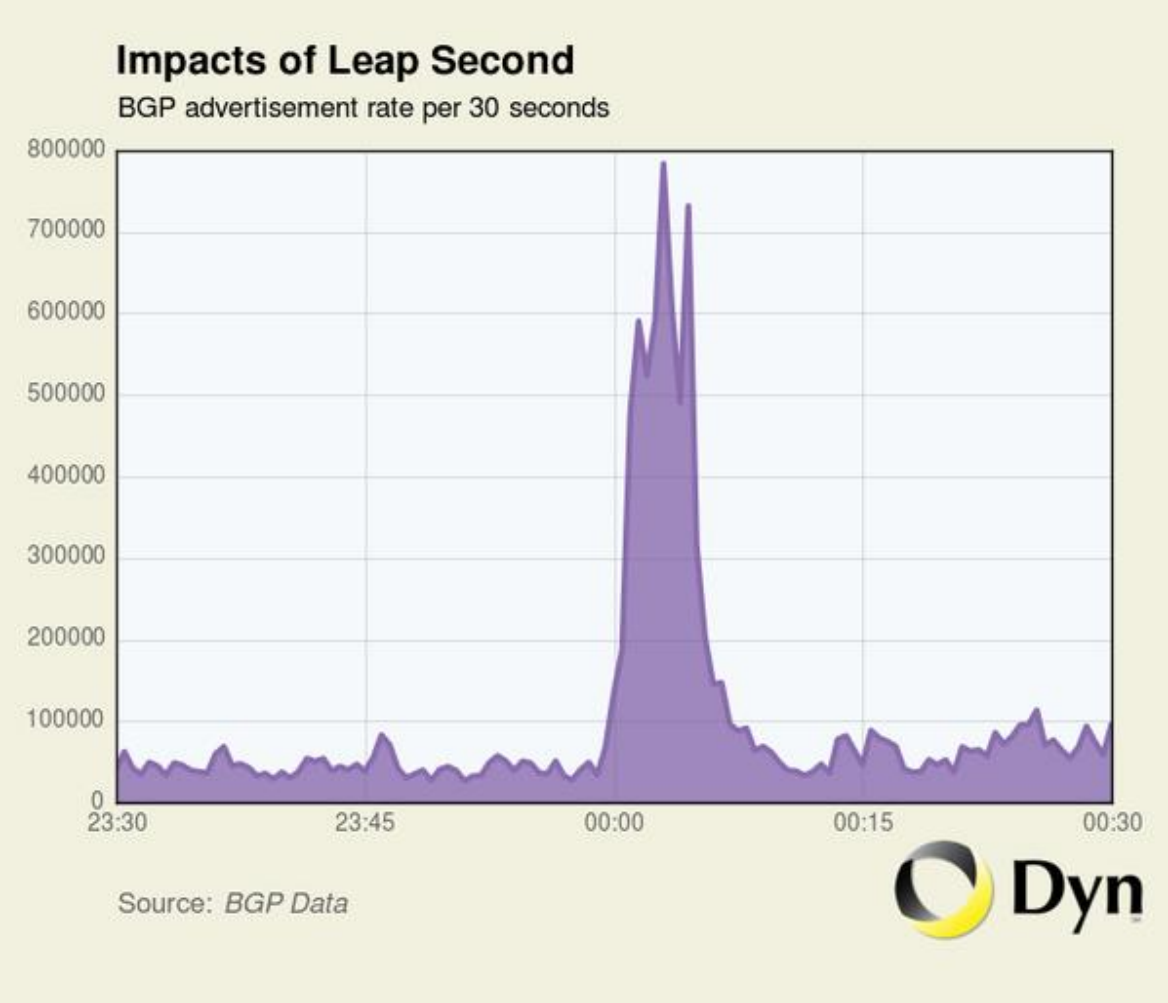
内容

- 最近流行しているハイジャック
- 肥大化する経路情報と注意喚起
- うるう秒2015
- その他国際動向

2015年のうるう秒

- ７月１日、3年ぶりに「うるう秒」挿入。8時59分60秒。
  - 時刻同期の方法は大きく2通り
    - Libitが挿入されたNTPサーバを参照し、1秒挿入する方法（stepモード）
    - 特定の時刻より継続的に徐々に時刻を微修正し、7月1日9時に向けて調整する方法（slewモード、アジャスト機能）
  - 3年前に比べると大きな被害はなかったが、未だに問題は起きている
    - 特定メーカーの機器がLIbitを参照するとカーネルパニックが発生
    - カーネル不具合でCPU使用率が高騰しwatchdogで再起動など
    - 世界中で約2000のネットワークで9時0分～5分程度の間ダウンが観測された
  - 11月に世界無線通信会議（WRC-15）で存続or廃止が検討される予定 700年で30分のずれ。日本は廃止派
    - ただし仮に今回廃止になったとしても次回からうるう秒対応がすぐに無くなるかは不明
- 一部のネットワークでも障害が発生し、不意な装置の再起動等によりBGP Updateの急増が観測された
  - 通常時の約10倍程度
  - アップデートが増加すると、BGPプロセスの処理に影響する

Leap second causes ~5 minutes of transient global routing instability



これは、、、

平素は当社サービスをご利用いただきありがとうございます。

7月1日(水)、お客様にご利用いただいております[redacted]/VPSの
一部におきまして、カーネルパニックが発生したため
7月1日午前9時0分から9時7分にホスト機を再起動いたしました。
インスタンスは順次起動いたしております。
全インスタンスの起動が完了いたしましたら改めてご連絡いたします。

お客様にはご迷惑をお掛けし、申し訳ございません。

■ 障害詳細
1.障害発生時間：7月1日(水)午前9時0分 ～
2.発生原因：原因につきましてはわかりかねました。
3.影響範囲：[redacted]
4.影響内容：インスタンスへ接続できない状態が発生しております。

全体的には3年前より比較的平和？

3年前の記事より：http://d.hatena.ne.jp/sh2/20120702

・ミクシィ ：SNS
→Linuxカーネルのバグでサーバ通信障害で4時間停止
・Reddit ：リンク共有サイト
→Apache Cassandraのうるう秒に関する障害発生
・StumbleUpon ：Webレコメンデーションサービス
・Yelp ：レストランガイド
・foursquare ：SNSタイプの地理情報共有サービス
・LinkedIn ：ビジネス型SNS
・Mozilla ：ブラウザサービス

内容

- 最近流行しているハイジャック
- 肥大化する経路情報と注意喚起
- うるう秒2015
- その他国際動向

Hijack, RouteLeak関連事案

- 2014/12 シリアで（恐らく）アサド政権によるhijack
  - シリアテレコムから1400経路程度のルートが数分間広告
  - Note worthy networks that were affected include US DOD, Chicago Public Schools , Level3, Savis, Telstra, UPC Liberty Global, Comcast, Time Warner Cable, Tiscali UK, China Enterprise Communications, Internet2, Province of New Brunswick, Yandex, Rogers Communications, Uganda Telecom, Dell, Sanford Airport Authority, Kabel Deutschland, Red Hat, YOUTUBE, Iran Post Company, Etihad Atheeb Telecom Company, Akamai, Telefonica Germany and many more.
- 2015/3　イギリスへのトラフィックがウクライナ経由に
- 2015/3　INDOSAT hijack
  - More specific routeが検出
  - 2014年1月には、Googleの8.8.8.8やAkamai, Amazonなどを含む2800程度のPrefixを38分間hijack

Hijack, RouteLeak関連事案

- 2015/6 マレーシアのLeakで環太平洋地域の広範囲に遅延等影響
- 2015/7 AWS(Boston)が約40分程度 RouteLeakにより停止
- 2015/9 インド/イランからK-rootへの到達不能
- 2015/10 iTELがRullRouteをoriginate
- 2015/11 インドからハイジャック

- Google's extensive peering likely insulated it from some of the effects of having its routes leaked. However, it didn't escape the incident completely unscathed. Here is an example of a normal traceroute to Google's data center in Council Bluffs, Iowa from Prague, which goes via Frankfurt and London before crossing the Atlantic Ocean.
- trace from Prague to Google, Council Bluffs, IA at 02:45 Jun 11, 2015

```
1  *
2  212.162.8.253    ge-6-14.car2.Prague1.Level3.net     16.583
3  4.69.154.135     ae-3-80.edge3.Frankfurt1.Level3.net 22.934
4  4.68.70.186      Level 3 (Frankfurt, DE)             23.101
5  209.85.241.110   Google (Frankfurt, DE)              23.796
6  209.85.250.143   Google (Frankfurt, DE)              24.086
7  72.14.235.17     Google (London, GB)                 32.709
8  209.85.247.145   Google (New York City)              103.091
9  216.239.46.217   Google (Council Bluffs)             133.098
10 209.85.250.4     Google (Council Bluffs)             133.245
11 216.239.43.217   Google (Council Bluffs)             133.536
12 *
13 74.125.142.192   Google (Council Bluffs)             132.643
```

2015/6
マレーシアのLeakで環太平洋地域の広範囲に遅延等影響

- During the routing leak, traces were redirected to Hong Kong (where Telekom Malaysia gets Level 3 transit) and across the Pacific Ocean for a performance hit of almost 400ms.
-

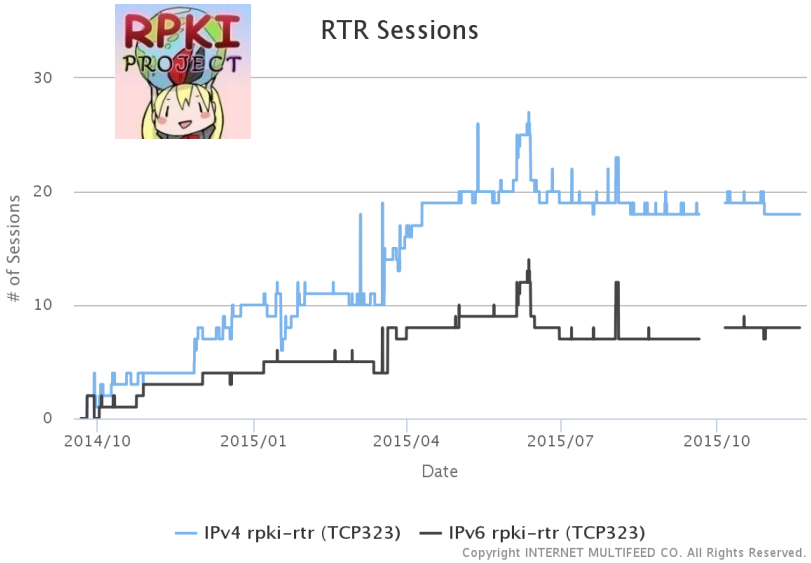
trace from Prague to Google, Council Bluffs, IA at 09:04 Jun 12, 2015

```
1  *
2  212.162.8.253    ge-6-14.car2.Prague1.Level3.net              41.213
3  *
4  67.17.134.242    telekom-malaysia-berhad.xe-0-2-0.ar2.clk1.gblx.net 451.264
5  *
6  209.85.242.242   Google (Mountain View)                       509.481
7  66.249.94.140    Google (Mountain View)                       482.303
8  64.233.174.176   Google (Mountain View)                       459.441
9  216.239.41.139   Google (Council Bluffs)                      457.846
10 72.14.239.48     Google (Council Bluffs)                      468.626
11 216.239.43.219   Google (Council Bluffs)                      456.841
12 *
13 74.125.142.192   Google (Council Bluffs)                      509.298
```


http://research.dyn.com/2015/06/global-collateral-damage-of-tmnet-leak/

RPKIの普及

- 国際的にも徐々に普及が進んでいる
  - 特にLACNIC, RIPE地域
- 日本国内でも、ちらほら登録方法や、誰が登録したらよいの？等の質問が増えてきた。
  - IRRはAS holder, RPKIはAddress holder



http://www.mfeed.ad.jp/rpki/roa_cache/statistics.html

10 records per page Search:

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	13721 (100%)	230 (1.68%)	14 (0.1%)	13477 (98.22%)	94.26%	1.78%
APNIC	153861 (100%)	3038 (1.97%)	1115 (0.72%)	149708 (97.3%)	73.15%	2.7%
ARIN	216330 (100%)	1698 (0.78%)	335 (0.15%)	214297 (99.06%)	83.52%	0.94%
LACNIC	76766 (100%)	14981 (19.52%)	689 (0.9%)	61096 (79.59%)	95.6%	20.41%
RIPE NCC	155033 (100%)	16280 (10.5%)	1205 (0.78%)	137548 (88.72%)	93.11%	11.28%

http://rpki.surfnet.nl/perrir.html

まとめ

- 最近流行している経路ハイジャック
  - 局所的なもの、未使用アドレス空間を狙ったもの
  - 身近なモニタリング手法から対策可
- 経路も依然増大している
  - 不意な増加や異常状態にも対応できる準備を
  - 自分の機器の確認を
- うるう秒2015は概ね無事に終了
  - 経路増加も観測された
- 世界では様々なセキュリティ事例がある
  - RPKIの普及にも注目