実践！ルーティングセキュリティ

ルーティングセキュリティ事例紹介と解説

KDDI株式会社
中野 達也

もくじ

1. 利用中の経路をハイジャックされた
2. 他者の経路を広報(広告)してしまった
3. 広報しようとしたら、なぜか使われていた
4. まとめ

KDDI株式会社 - All Rights Reserved

1.利用中の経路をハイジャックされた

何が起きる?
気づくには?
どうやって対応しよう?

何が起こる?

- トラフィックの急落

- 名前解決、Web閲覧、メール送受信NG
- お客様からの不通問い合わせ

ただし、これらに気づけないことも

KDDI株式会社 - All Rights Reserved

気づくには?

検知システムを使ってみる

BGPMON	http://bgpmon.net/
Cyclops	http://cyclops.cs.ucla.edu/
ISAlarm(RIPE)	https://www.ripe.net/is/alarms/
Renesys	http://www.renesys.com/
経路奉行	http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html

KDDI株式会社 - All Rights Reserved

検知システムの比較

	経路奉行	BGPmon	Cyclops	IS Alarms	Renesys
経路の情報源	国内ISPの経路情報	RIPE-RIS Route views		RIPE-RIS	More than 360 sites
情報源との比較方法	JPIRR	ユーザ入力情報			
通知、確認方法	メール	Web メール SMS	Web メール RSS	Web メール Syslog	Web
備考	JPIRRにObject登録で監視対象 X-keiro登録で通知対象	有料 (5prefixまでは無料) ROA対応らしい	事前登録要 ASNでPrefixも登録可 MITM検知	事前登録要 Prefix手入力 MITM検知	有料

KDDI株式会社 - All Rights Reserved

検知システム - BGPMON

- 2012年10月から有料になった

http://www.bgpmon.net/new-version-of-bgpmon-net/

監視対象数	月額	年額
5Prefixまで	無料	無料
10Prefix以上	$39	$429
20Prefix以上	$59	$649
50Prefix以上	$89	$979
100Prefix以上	$129	$1419
250Prefix以上	$249	$2739
500Prefix以上	$449	$4939
1000Prefix以上	$849	$9339

(BGPMONのサイトより引用)

KDDI株式会社 - All Rights Reserved

検知システム - 経路奉行

- 経路ハイジャック通知実験メール
  - JPIRRにRouteオブジェクトを登録していること
  - かつ、Route/maintオブジェクトのdescrに X-Keiroを設定していること

（メール例）
ご担当者様

以下の通り、経路ハイジャックが疑われる状態を検知しました。

```
----------------------------------------
検知日時                    : Fri 28 Mar 2008 10:50:30 +0900
Routeオブジェクト           : 192.0.2.0/24
RouteオブジェクトのOrigin   : AS2515
検知したPrefix              : 192.0.2.0/24
----------------------------------------
```


KDDI株式会社 - All Rights Reserved

X-keiro

- JPIRRのroute or maint objectのdescrに書く

```
(whois 記入例)
> whois -h jpirr.nic.ad.jp MAINT-AS2515
mntner:      MAINT-AS2515
descr:       Japan Network Information Center
             People authorized to make changes for AS2515
             X-Keiro: okadams@nic.ad.jp
             X-Keiro: kawabata@nic.ad.jp
(以下省略)
```

参考サイト　http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html
http://www.nic.ad.jp/doc/jpnic-01077.html

KDDI株式会社 - All Rights Reserved

どうやって対応しよう? (1)

- 広報元を突き止め、止めてもらう
  - show ip bgp <prefix>　　広報元の確認
  - traceroute　　結果の確認
    - 自ASルータで
    - Looking Glass / traceroute.orgで
  - RouteViewsのmrtdump archiveを参照

KDDI株式会社 - All Rights Reserved

どうやって対応しよう?(2)

- 広報元の連絡先を調べて、連絡を試みる
  - Whoisで調べてみる
    - JPNIC Whois ,RADB …etc
    - mnt-byやグループハンドル等も参照する
  - PeeringDBを参照する
    - https://www.peeringdb.com/
  - HurricaneElectricのBGP Toolkitを参照する
    - http://bgp.he.net/

KDDI株式会社 - All Rights Reserved

広報元への問い合わせ方

- noc、peering、admin等のアドレスにも送ってみる
- 事実を淡々と書くにとどめる
  テンプレートを作っておくと早いかも
- Looking Glass / IRRで得た結果等を張り付けるとよい

返事がない・知らないと言われた場合

上位ASに相談してみる

- 広報元のさらに上位にあるASに
  コンタクトを取ってみる

KDDI株式会社 - All Rights Reserved

取り返す?

- 権威のない広報を行っているASのPrefixよりも
  さらに細かいPrefixを広報して取り返す

でも・・・

address maskフィルタに引っかかるかも

取り返すときに設定をミスしたら加害者になりうる

根本的な解決方法は
誤った広報を停止させること

KDDI株式会社 - All Rights Reserved

最後の手段

- janogやnanogのMLに現状を説明してみる
  - 同じようなASが他にもいるかも
  - その情報が、解決の糸口になるかも?

解決できた事例も

KDDI株式会社 - All Rights Reserved

2.他者の経路を広報(広告)してしまった

やってしまったら

何が起こる?

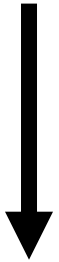
- トラフィックの急増
- 不正アクセスの急増
- 被害側からの問い合わせ等

しかも、やった側は気づけない場合が多い

KDDI株式会社 - All Rights Reserved

なぜ起きるか (1)

タイプミス?と思われる事例あり



外から見れば故意/過失は関係ない

IPv6化が進むと増えるかも?

KDDI株式会社 - All Rights Reserved

なぜ起きるか (2)

狙われやすいpfefixだったり

- 同じ数字の羅列
  例：111.111.111.0/24、12.12.12.0/24

- 数字として連続している
  例： 12.34.56.0/24、98.76.54.0/24

練習、検証等で生成した経路を誤広報・・?

KDDI株式会社 - All Rights Reserved

やった側は気づけない・・・どうする?

やってしまった側は、なかなか気づけない
(さっきも書いたけど)

教えてもらえる環境作りが必要

- そのために
  - whois,JPIRR/RADBの定期的な更新
  - peeringDBの確認・更新(できれば)

KDDI株式会社 - All Rights Reserved

3.使おうとしたら、何故か使われていた

何が起きた?

- IPアドレスを割り振られたので使おうとした
  → 何故か他のASから広報されている

- どうやって対処したか
  → STNet 高橋さんにお話しいただきます

KDDI株式会社 - All Rights Reserved

4.まとめ

今からでもできること

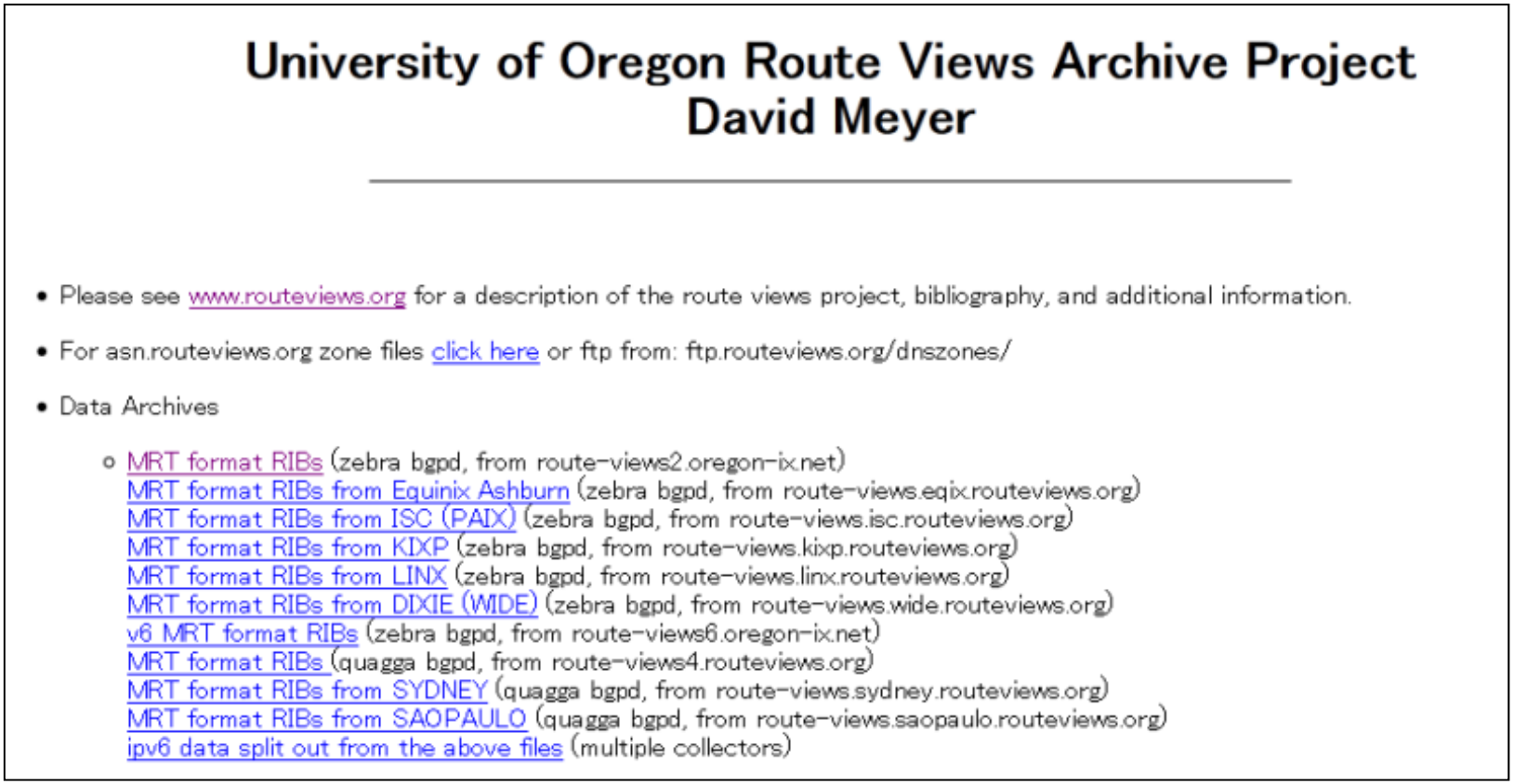
まとめ

- 身近で起きた時に
  - 何が起こるか理解しておく
  - 何をするべきか決めておく
- なによりも気づくことができるように
  - 検知する手段を構築する
- やってしまった時に、教えてもらえるように
  - 各種問い合わせ先はしっかり更新する

KDDI株式会社 - All Rights Reserved

参考：mrtdumpの取得

Route Views Archive http://archive.routeviews.org/



University of Oregon Route Views Archive Project
David Meyer

- Please see www.routeviews.org for a description of the route views project, bibliography, and additional information.
- For asn.routeviews.org zone files click here or ftp from: ftp.routeviews.org/dnszones/
- Data Archives
  - MRT format RIBs (zebra bgpd, from route-views2.oregon-ix.net)
    MRT format RIBs from Equinix Ashburn (zebra bgpd, from route-views.eqix.routeviews.org)
    MRT format RIBs from ISC (PAIX) (zebra bgpd, from route-views.isc.routeviews.org)
    MRT format RIBs from KIXP (zebra bgpd, from route-views.kixp.routeviews.org)
    MRT format RIBs from LINX (zebra bgpd, from route-views.linx.routeviews.org)
    MRT format RIBs from DIXIE (WIDE) (zebra bgpd, from route-views.wide.routeviews.org)
    v6 MRT format RIBs (zebra bgpd, from route-views6.oregon-ix.net)
    MRT format RIBs (quagga bgpd, from route-views4.routeviews.org)
    MRT format RIBs from SYDNEY (quagga bgpd, from route-views.sydney.routeviews.org)
    MRT format RIBs from SAOPAULO (quagga bgpd, from route-views.saopaulo.routeviews.org)
    ipv6 data split out from the above files (multiple collectors)

KDDI株式会社 - All Rights Reserved

参考：mrtdumpの参照

例

bgpdump (mrtfile) | grep ‘prefix'
bgpdump (mrtfile) | grep '^ASPATH:' | more | sort | uniq
bgpdump -M (mrtfile) |grep (prefix) | grep "|A|" | awk -F "¥|" '{print $2,$6,$7}'

```
$ bgpdump  (mrtfile)
TIME: 11/15/11 06:00:17
TYPE: BGP4MP/MESSAGE/Update
FROM: 4.69.184.193 AS3356
TO: 128.223.51.102 AS6447
ORIGIN: IGP
ASPATH: 3356 286 8607 12654
NEXT_HOP: 4.69.184.193
MULTI_EXIT_DISC: 0
AGGREGATOR: AS64614 10.18.173.65
COMMUNITY: 3356:3 3356:22 3356:86 3356:575 3356:666 3356:2011
ANNOUNCE
  84.205.65.0/24

$ bgpdump –M (mrtfile)
BGP4MP|11/15/11 06:00:17|A|64.71.255.61|812|204.62.208.0/24|812 3549 1239|IGP
```

bgpdumpのソース　　http://www.ris.ripe.net/source/bgpdump/

KDDI株式会社 - All Rights Reserved