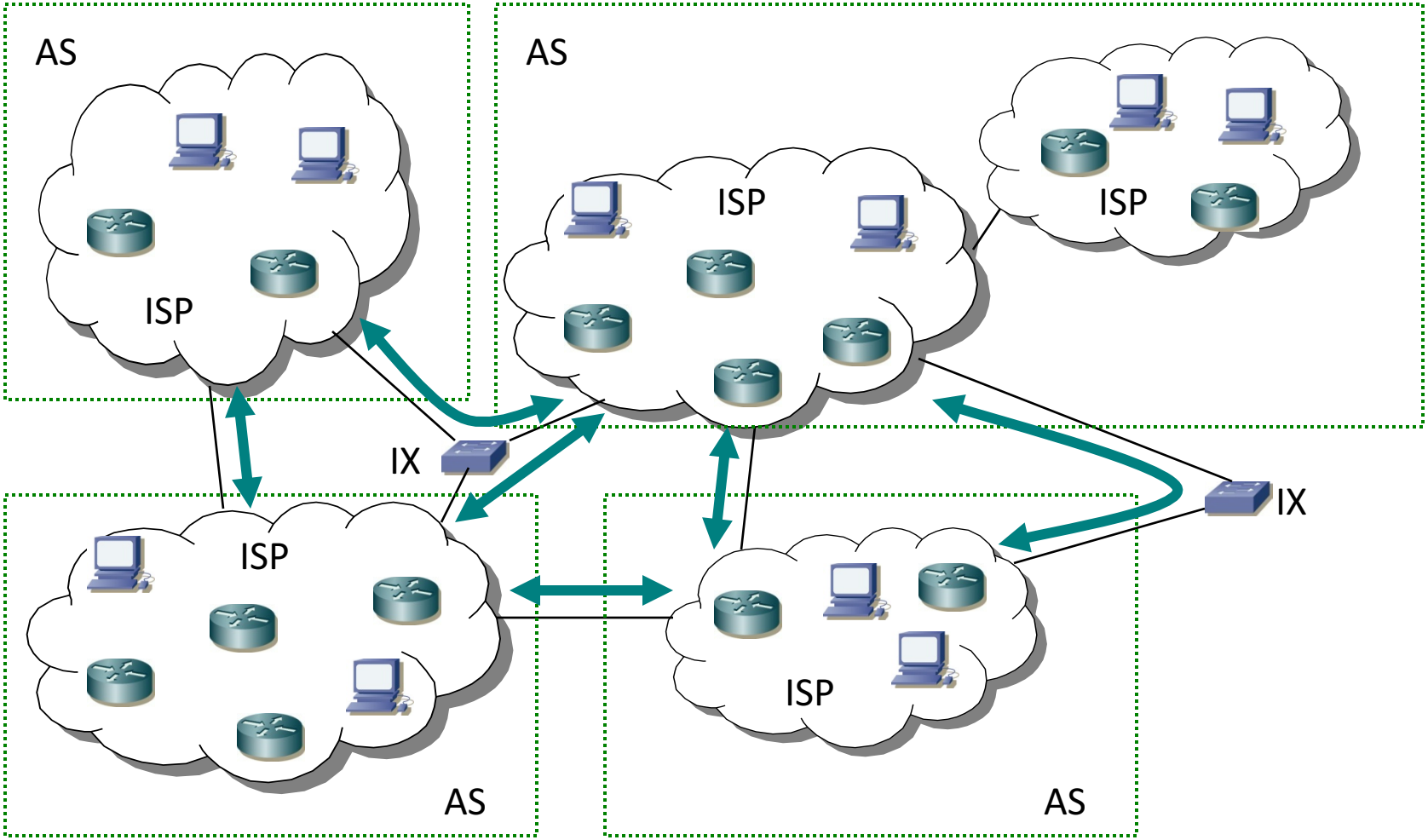
BGP route hijacking

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

IP address

- Most abuse reports are based on source IP address, as it’s considered as the identifier and the locator of the corresponding host on the internet.
- But it’s not always true...

BGP?



Mis-announcements

- BGP announcements without authority
  - Mostly it's believed as mistakes like typo, leakage of test and other mis-configurations
  - We are observing a bunch of this stuff
- It has been said there are intentional BGP hijacking by malicious folks, and here is the cases….

Starting with a post to JANOG ML

- [janog:12845] IIJ to the white courtesy phone.
  - Notifying strange BGP announcements
  - Also stating the prefix was listed at the Spamhaus SBL

- Thanks for the heads-up!

The /16 IPv4 prefix

- Transferred to IIJ recently
  - on 21/Oct/2014
- IIJ kept it in stock for future use
  - IIJ didn't start to announce it at that time ☹
  - WHOIS information at JPNIC was updated, but no IRR registration ☹
- An ISP in U.S. started to announce the IP block as 2 x /17s on 5/Jan/2015
  - No, IIJ didn't ask that

To stop the wrong announcements

- IIJ contacted the announcing ISP immediately
  - E-mail to their NOC followed by a phone call
  - Started BGP announcements by ourselves
- The first contact:
  - Got ACK and the person on the call agreed to deal with the announcements, but nothing was happened in the next 48 hours
- The second contact:
  - Convinced the (different) person on the call, and got a ticket # to track the progress of handling
  - The announcements were finally stopped ☺

Lesson learned #1

- Ask for a ticket #
  - especially in case the ISP has a ticket system to track their jobs
- Keep WHOIS DB up-to-date
  - To prove your correctness
  - I sent our WHOIS information to the NOC by e-mail, and also asked the NOC person to query the prefix by himself

The progress

- 4/Feb/2015 - The post to JANOG
  - The first contact to the ISP
- 6/Feb/2015 - The second contact to the ISP
- 7/Feb/2015 - The routes were withdrawn
- 12/Feb/2015 - Contacted Spamhaus to delist
- 13/Feb/2015 - The prefix was delisted from SBL

Bringing in IP spaces to ISP

- A customer of the ISP submitted a LoA (Letter of Authority) to use the prefix, and asked the ISP to originate the BGP announcements

- No, IIJ didn't submit such a document

An Example of Letter of Authority

<Company Name>
<Address>

<date>

To: <the Customer>

We authorize <the Customer> or <the ISP> to announce the following IP blocks -

<IP address blocks>

This authorization shall be valid until revoked by us in writing or by e-mail from <e-mail address>.

I may be contacted at <Tel#> or <e-mail address>

Sincerely,

<signature>

<signer's name in print>

<Company Name>

The actual LoA looks ... strange

- The company name was a family company of the previous resource holder
- Suspicious
  - The domain name used as a contact e-mail address was different from the actual one
    - The domain name was newly registered in 2014
  - The Tel# was wrong - missing a country code
    - As the previous holder registered it wrongly at the whois DB before

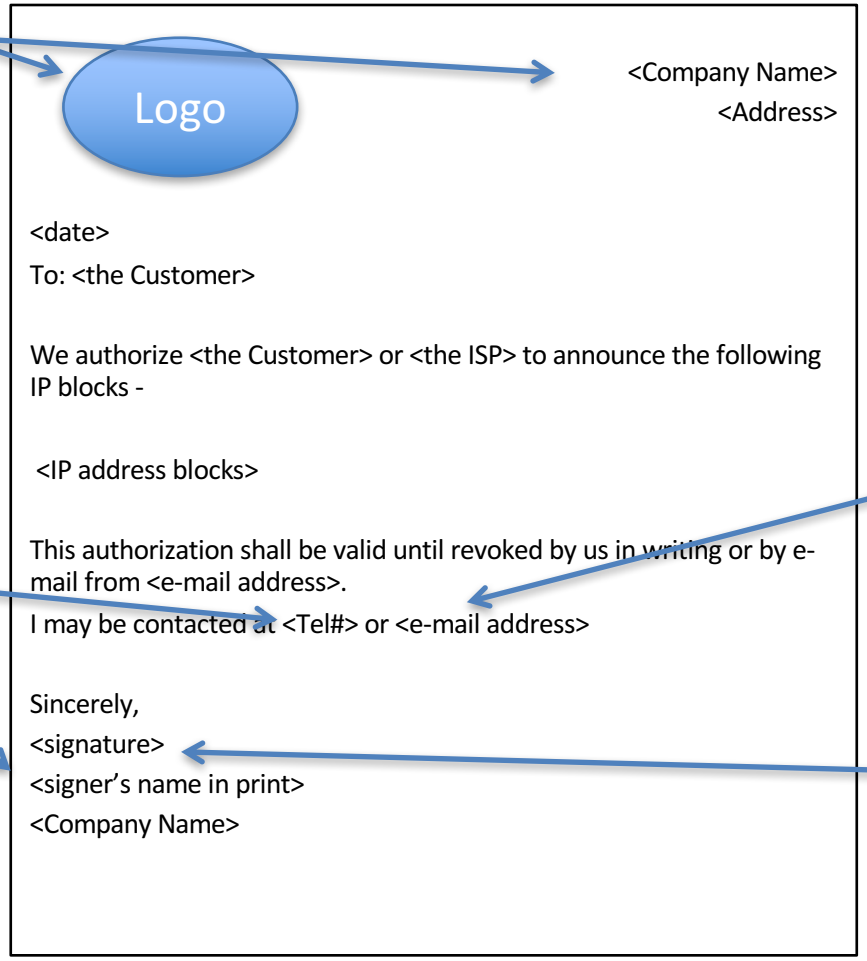
Visited the previous resource holder

- Met a person who was previously the contact person of their whois DB entry
  - and also his name was used as a signer in the LoA
- No, he didn't sign the document, and their company wasn't aware of the LoA and even the domain name which was used in the LoA

- A fake LoA!!

The fake LoA

Copied from a web site of a family company of the previous resource holder

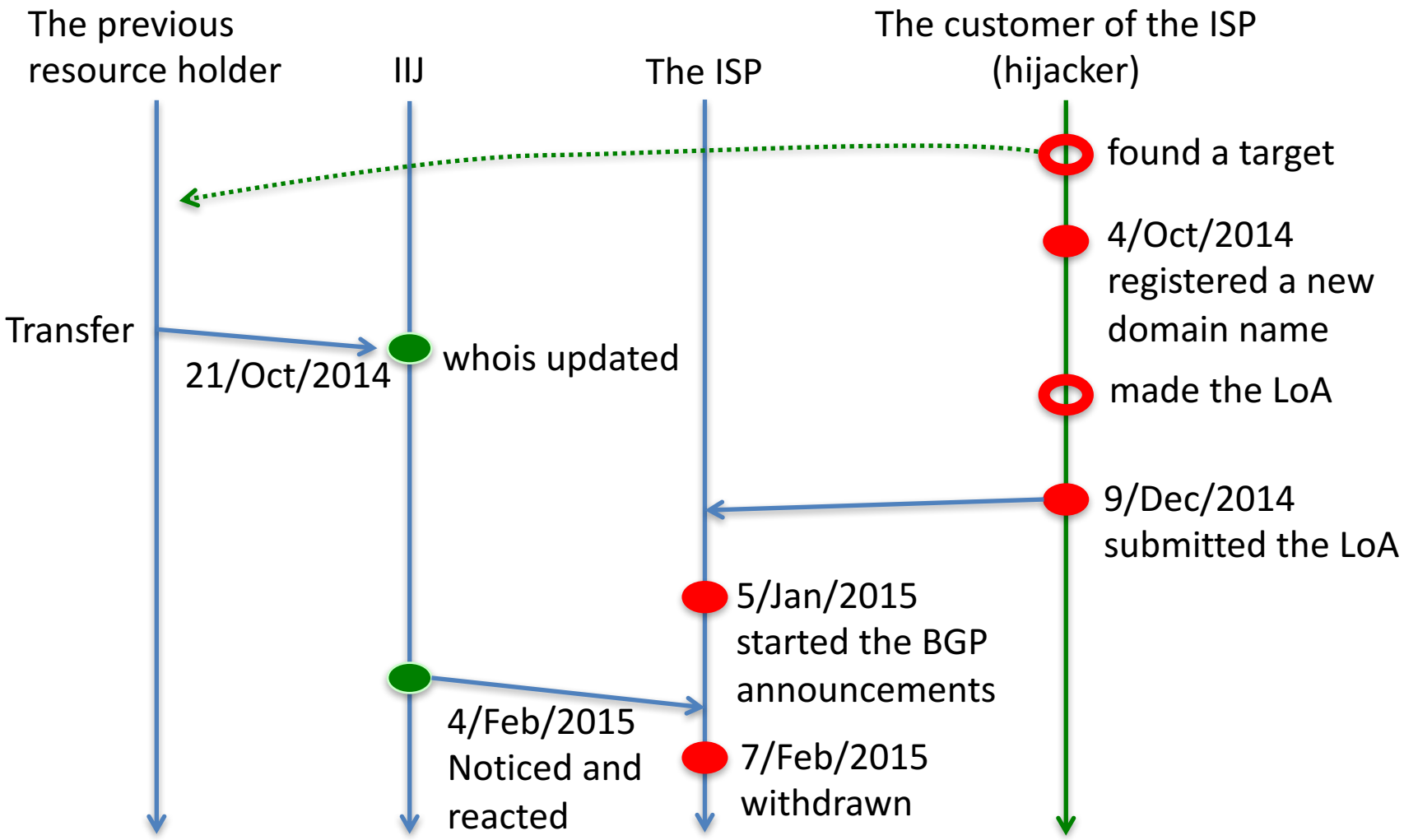


Registered a new domain name looks like related to the organization

Copied from previous whois DB entry

A fake signature

Timeline


The previous resource holder
IIJ
The ISP
The customer of the ISP (hijacker)
found a target
4/Oct/2014 registered a new domain name
made the LoA
Transfer
21/Oct/2014
whois updated
9/Dec/2014 submitted the LoA
5/Jan/2015 started the BGP announcements
4/Feb/2015 Noticed and reacted
7/Feb/2015 withdrawn

The hijacker

- We don’t know how they used the network
  - No evidence so far
  - No spam compliant related to the prefix
- After stopping the announcement, they started to use ‘the next’ prefix by using the same technique - by submitting a fake LoA ☹
  - It was noticed and stopped by the actual resource holder a few months later

Another case

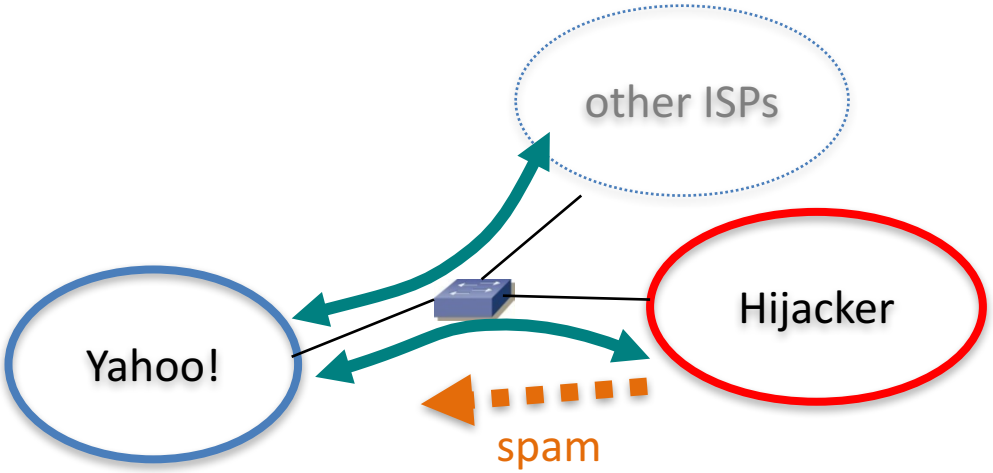
- Invisible Hijacking
  - https://ripe72.ripe.net/presentations/45-Invisible_Hijacking.pdf
- Started to receive reports from spamcop
  - it continued even though they put filter whole outbound port 25

Not in the global routing table

- They checked with public looking-glass services like RIPE RIS and route-views
  - No suspicious announcement
- A clue, all reports were related to Yahoo! mail
  - Contacted the Yahoo! and finally found suspicious BGP announcements

IXP

- The hijacker established a peering with Yahoo! at IXP and announced more specifics to get a reachability (to the Yahoo! network only)



How is this possible?

- Becoming a customer is easy
  - as long as the customer pays, most operators are happy with that
- Spoofing ASN at IXP is easy
  - IXP is providing simple L2 service, so they don't care which ASNs and prefixes are used to exchange routing information
- Open peering policy also helps
  - some big operators have an open peering policy, and happy to peer with anyone at IXPs

The current situation

- Ran out IPv4 Free Space
  - getting difficult to get enough IPv4 space
- IP reputation database
  - to avoid access from/to malicious activities

- Aaaaah, the situation probably motivates malicious folks to hijack a prefix more and more...

Weak points

- Customers bringing in their IP space
  - WHOIS, RPKI?
- Transit customers
  - WHOIS, IRR?, RPKI?
- Peering partners
  - IRR?, RPKI?

Summary

- Intentional BGP-hijacking are happening
  - Hijackers pay money to buy a network service
  - People assume some kind of implicit trust relationship for customers, hijacker use the trust to convince others to announce their BGP announcements
- We need a strong infrastructure to prove our number resources

BACKUP slides

looking back

- IIJ should announce all holding prefixes
  - We changed our policy to announce all of them
  - Before announcements, IIJ registers route objects to IRRs - JPIRR and RADB. By registering a route object at JPIRR, a route monitoring service named ‘keiro bugyo’ automatically starts to monitor malicious announcement related to the route object. ☺
- The ISP should carefully check IP blocks before announcements
  - As whois DB was already changed - indicating IIJ as a resource holder at that time

WHOIS

- WHOIS command
  - Which WHOIS server should I use for starting?
    - whois.iana.org ?
  - Modern command hopefully handles it well
  - Are you familiar with CLI? windows users?
- Web based WHOIS gateway
  - Which one should I use?
    - Starting with http://whois.iana.org/ ?

finding a resource holder by WHOIS

- IANA -> RIR -> (NIR ->) LIR
  - Think about regions which do not have NIRs, and probably some people are not aware of it
- Allocations and Assignments
  - Can you distinguish these on whois?
- ERXs and inter-RIR transfers
  - IANA -> RIR -> RIR -> (NIR ->) LIR
  - It seems each IR uses own expression to indicate a reference for further information

whois at IANA

```
$ whois -h whois.iana.org '160.13.0.0'
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:        whois.arin.net

inetnum:      160.0.0.0 - 160.255.255.255
organisation: Administered by ARIN
status:       LEGACY

whois:        whois.arin.net

changed:      1993-05
source:       IANA
```

whois at ARIN

```
$ whois -h whois.arin.net '160.13.0.0'

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#


#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 160.13.0.0"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
#
http://whois.arin.net/rest/nets;q=160.13.0.0?showDetails=true&showARIN=false&showNonArinTopLeve
lNet=false&ext=netref2
#

NetRange:       160.11.0.0 - 160.30.255.255
CIDR:           160.24.0.0/14, 160.11.0.0/16, 160.30.0.0/16, 160.28.0.0/15, 160.12.0.0/14, 160.16.0.0/13
NetName:        APNIC-ERX-160-11-0-0
NetHandle:      NET-160-11-0-0-1
Parent:         NET160 (NET-160-0-0-0-0)
NetType:        Early Registrations, Transferred to APNIC
OriginAS:
Organization:   Asia Pacific Network Information Centre (APNIC)
RegDate:        2004-04-05
Updated:        2009-10-08
Comment:        This IP address range is not registered in the ARIN database.
Comment:        This range was transferred to the APNIC Whois Database as
Comment:        part of the ERX (Early Registration Transfer) project.
Comment:        For details, refer to the APNIC Whois Database via
Comment:        WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment:
Comment:        ** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment:        for the Asia Pacific region.  APNIC does not operate networks
Comment:        using this IP address range and is not able to investigate
Comment:        spam or abuse reports relating to these addresses.  For more
Comment:        help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
Ref:            http://whois.arin.net/rest/net/NET-160-11-0-0-1

ResourceLink:  http://wq.apnic.net/whois-search/static/search.html
ResourceLink:  whois.apnic.net

OrgName:        Asia Pacific Network Information Centre
OrgId:          APNIC
Address:        PO Box 3646
City:           South Brisbane
StateProv:      QLD
PostalCode:     4101
Country:        AU
RegDate:
Updated:        2012-01-24
Ref:            http://whois.arin.net/rest/org/APNIC

ReferralServer:  whois://whois.apnic.net
ResourceLink:  http://wq.apnic.net/whois-search/static/search.html

OrgAbuseHandle: AWC12-ARIN
OrgAbuseName:   APNIC Whois Contact
OrgAbusePhone:  +61 7 3858 3188
OrgAbuseEmail:  search-apnic-not-arin@apnic.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/AWC12-ARIN

OrgTechHandle: AWC12-ARIN
OrgTechName:   APNIC Whois Contact
OrgTechPhone:  +61 7 3858 3188
OrgTechEmail:  search-apnic-not-arin@apnic.net
OrgTechRef:    http://whois.arin.net/rest/poc/AWC12-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#
```

whois at APNIC

```
$ whois -h whois.apnic.net '160.13.0.0'
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '160.13.0.0 - 160.13.255.255'

inetnum:        160.13.0.0 - 160.13.255.255
netname:        IIJ
descr:          Internet Initiative Japan Inc.
descr:          Iidabashi Grand Bloom,
descr:          2-10-2 Fujimi, Chiyoda-ku,
descr:          Tokyo, 102-0071 Japan
country:        JP
admin-c:        JNIC1-AP
tech-c:         JNIC1-AP
status:         ALLOCATED PORTABLE
remarks:        Email address for spam or abuse complaints : abuse-contact@iij.ad.jp
mnt-irt:        IRT-JPNIC-JP
mnt-by:         MAINT-JPNIC
mnt-lower:      MAINT-JPNIC
changed:        hm-changed@apnic.net 20050712
changed:        ip-apnic@nic.ad.jp 20141021
source:         APNIC

irt:            IRT-JPNIC-JP
address:        Urbannet-Kanda Bldg 4F, 3-6-2 Uchi-Kanda
address:        Chiyoda-ku, Tokyo 101-0047, Japan
e-mail:         hostmaster@nic.ad.jp
abuse-mailbox:  hostmaster@nic.ad.jp
admin-c:        JNIC1-AP
tech-c:         JNIC1-AP
auth:           # Filtered
mnt-by:         MAINT-JPNIC
changed:        abuse@apnic.net 20101108
changed:        hm-changed@apnic.net 20101111
changed:        ip-apnic@nic.ad.jp 20140702
source:         APNIC

role:           Japan Network Information Center
address:        Urbannet-Kanda Bldg 4F
address:        3-6-2 Uchi-Kanda
address:        Chiyoda-ku, Tokyo 101-0047,Japan
country:        JP
phone:          +81-3-5297-2311
fax-no:         +81-3-5297-2312
e-mail:         hostmaster@nic.ad.jp
admin-c:        JI13-AP
tech-c:         JE53-AP
nic-hdl:        JNIC1-AP
mnt-by:         MAINT-JPNIC
changed:        hm-changed@apnic.net 20041222
changed:        hm-changed@apnic.net 20050324
changed:        ip-apnic@nic.ad.jp 20051027
changed:        ip-apnic@nic.ad.jp 20120828
source:         APNIC

% Information related to '160.13.0.0 - 160.13.15.255'

inetnum:        160.13.0.0 - 160.13.15.255
netname:        IIJNET
descr:          IIJ Internet
country:        JP
admin-c:        JP00010080
tech-c:         JP00010080
remarks:        This information has been partially mirrored by APNIC from
remarks:        JPNIC. To obtain more specific information, please use the
remarks:        JPNIC WHOIS Gateway at
remarks:        http://www.nic.ad.jp/en/db/whois/en-gateway.html or
remarks:        whois.nic.ad.jp for WHOIS client. (The WHOIS client
remarks:        defaults to Japanese output, use the /e switch for English
remarks:        output)
changed:        apnic-ftp@nic.ad.jp 20150417
changed:        apnic-ftp@nic.ad.jp 20150424
source:         JPNIC

% This query was served by the APNIC Whois Service version 1.69.1-APNICv1r7-SNAPSHOT (WHOIS4)
```

whois at JPNIC

```
$ whois -h whois.nic.ad.jp '160.13.0.0 /e'
[ JPNIC database provides information regarding IP address and ASN. Its use   ]
[ is restricted to network administration purposes. For further information,  ]
[ use 'whois -h whois.nic.ad.jp help'. To only display English output,        ]
[ add '/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.      ]

Network Information:
a. [Network Number]           160.13.0.0/20
b. [Network Name]             IIJNET
g. [Organization]             IIJ Internet
m. [Administrative Contact]   JP00010080
n. [Technical Contact]        JP00010080
p. [Nameserver]               dns0.iij.ad.jp
p. [Nameserver]               dns1.iij.ad.jp
[Assigned Date]               2015/04/17
[Return Date]
[Last Update]                 2015/04/24 11:47:06(JST)

Less Specific Info.
----------
Internet Initiative Japan Inc.
                [Allocation]                  160.13.0.0/16

More Specific Info.
----------
No match!!
```

whois at JPNIC again

```
$ whois -h whois.nic.ad.jp '160.13.0.0/16 /e'
[ JPNIC database provides information regarding IP address and ASN. Its use   ]
[ is restricted to network administration purposes. For further information,  ]
[ use 'whois -h whois.nic.ad.jp help'. To only display English output,        ]
[ add '/e' at the end of command, e.g. 'whois -h whois.nic.ad.jp xxx/e'.      ]

Network Information:
[Network Number]              160.13.0.0/16
[Network Name]
[Organization]                Internet Initiative Japan Inc.
[Administrative Contact]      JP00010080
[Technical Contact]           JP00010080
[Abuse]                       abuse-contact@iij.ad.jp
[Allocated Date]              2014/10/21
[Last Update]                 2014/10/21 15:04:47(JST)

Less Specific Info.
----------
No match!!

More Specific Info.
----------
IIJ Internet
        IIJNET [Assignment]                   160.13.0.0/20
IIJ Internet
        IIJNET [Assignment]                   160.13.16.0/24
 [...]
```

allocations

- It’s already complicated
  - and getting more complicated
- IR whois is not so human friendly nor machine friendly
  - You need to train engineers about every whois DB’s expressions, history of the Internet, the current resource policies. Yes, it’s important though...
  - And probably that’s why we have IRRs to register routing related information
- We need something better to prove our holding resources

RPKI

- Public Key Infrastructure for Number Resources
  - Such as IP addresses and AS numbers
  - A digital certificate can prove that you are the current resource holder of specific number resource
  - You can add digital signature to your documents like LoA or transfer agreement
- You can issue ROAs to indicate originating AS for prefixes

lesson learned #2

- Announce all holding prefixes
  - Register route objects to an IRR for reference
- IR whois is ... complicated
  - Hierarchy, ERXs and transfers
  - Assignments and allocations in the same DB
- RPKI is the next choice for us
  - We need to promote RPKI more, and train engineers to be aware of public-key cryptography
  - Signing and verifying by using public-key cryptography is a key technology now days