ISP cache nameservers and BCP140

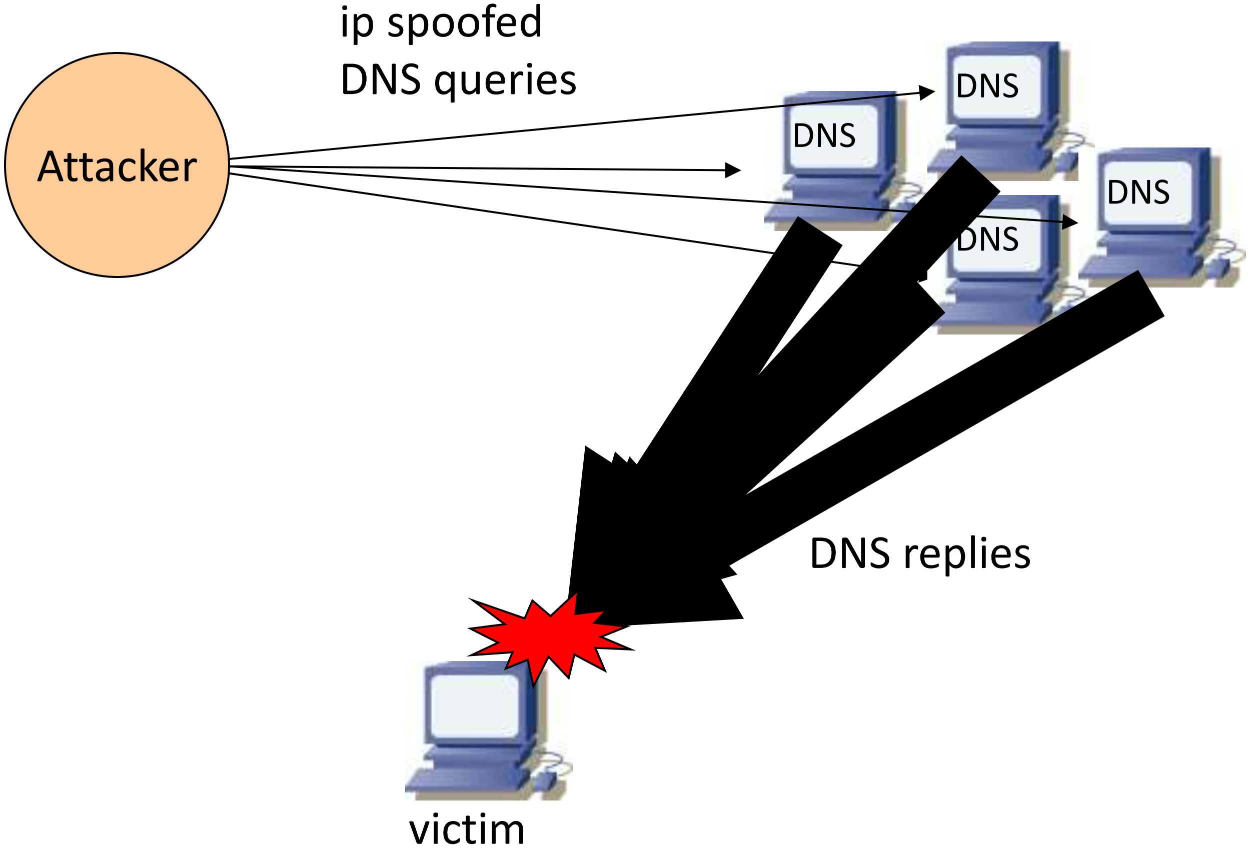
Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

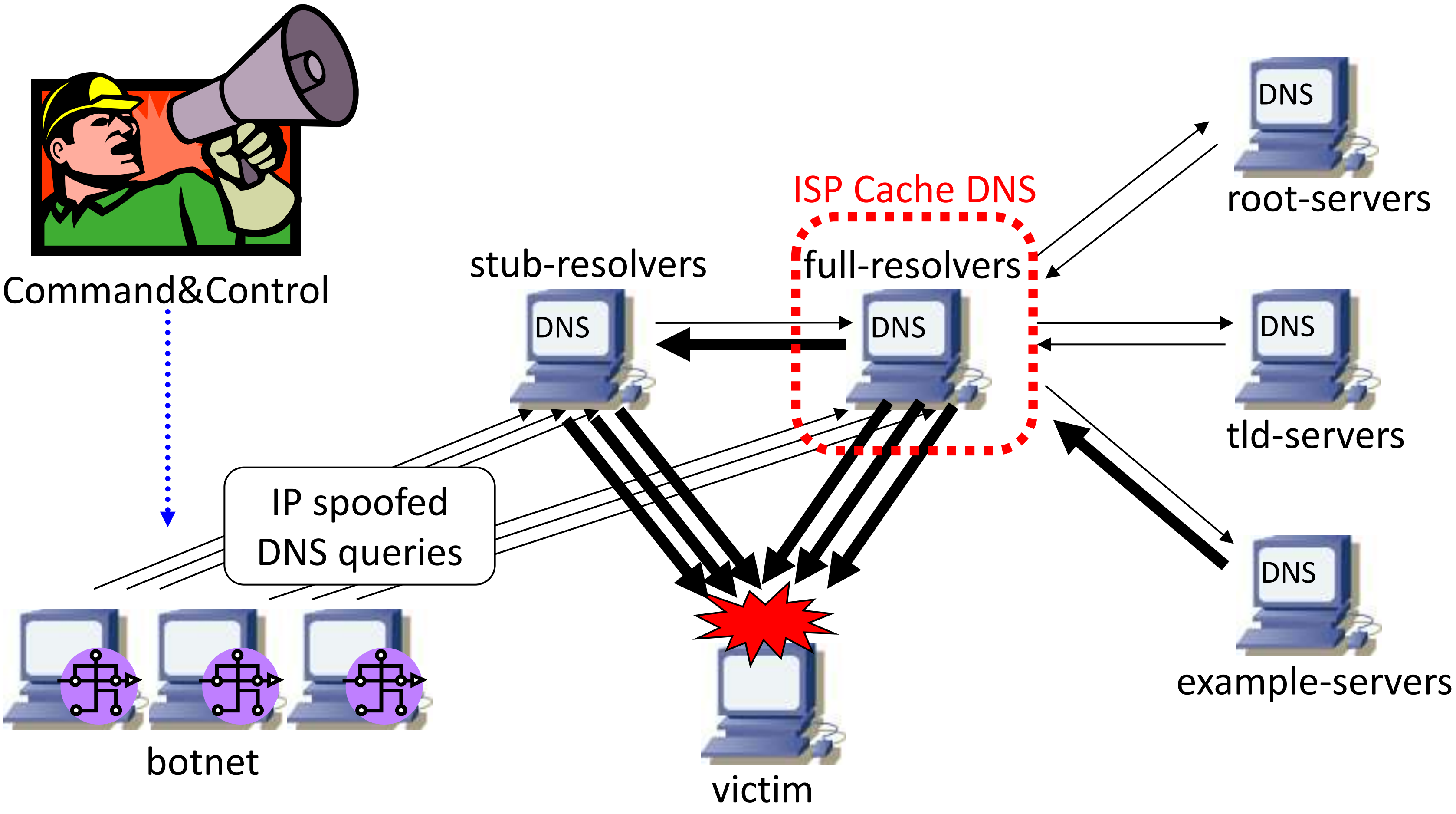
implementing BCP140

- Several ISPs in Japan has operated ‘open’ recursive nameservers for many years. As these servers tend to be used for dns amp attack, ISPs decided to put ACL to accept queries from its customers only - BCP140.

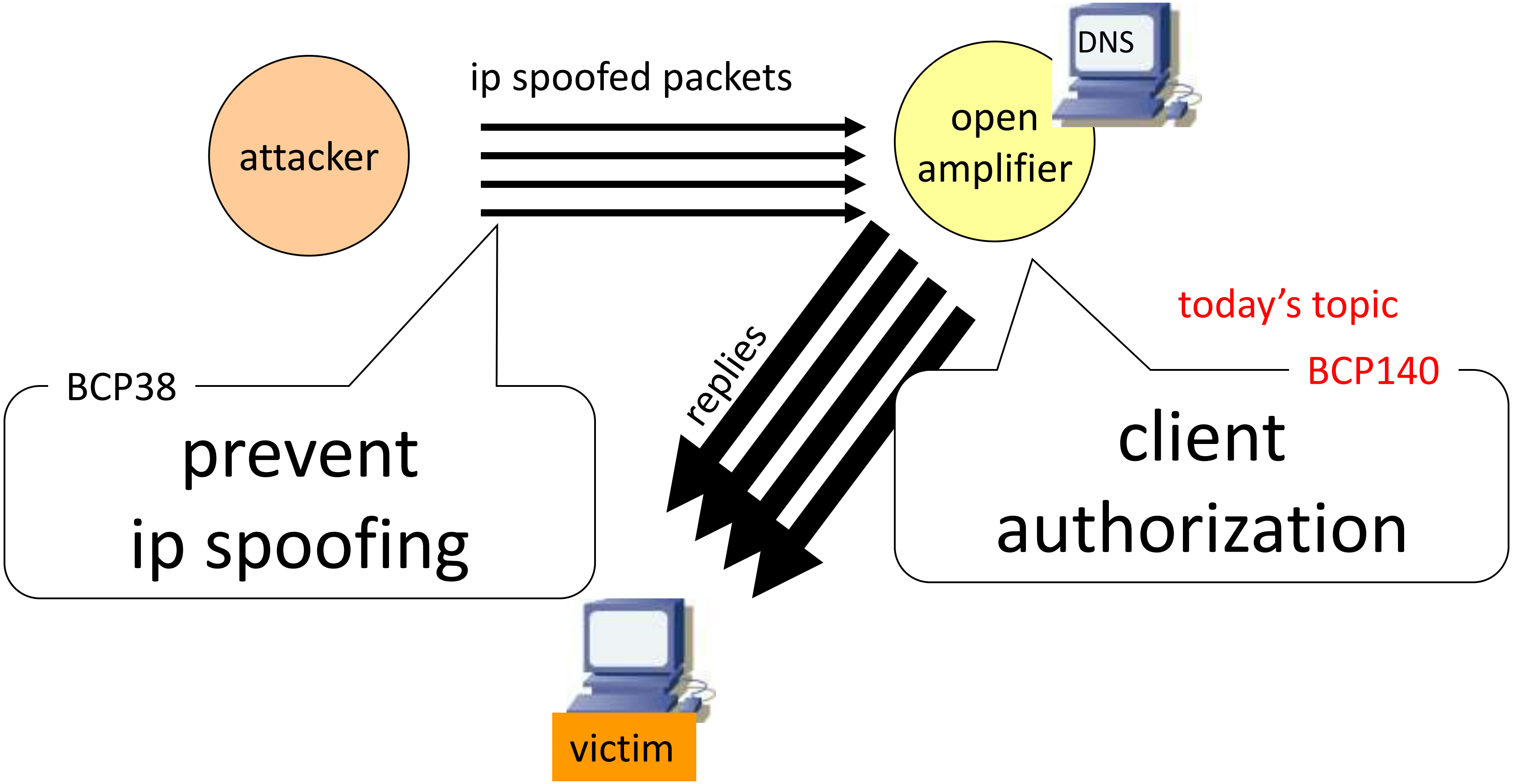
dns amplification attack



relations – dns amp attack



solutions against ip reflection attacks



BCP38

prevent ip spoofing

today's topic

BCP140

client authorization

Client Authorization

- BCP140 recommends several ways:
  1. source IP address based
  2. Incoming interface based
  3. TSIG/SIG(0) signed queries
  4. using a local caching nameserver
- The 1st one is the option for ISPs
  - no other choice at this moment
- source IP address based authorization
  - in other words, ACL ☺

Technically it’s quite easy

```
// BIND9 example
acl my-net { 192.0.2.0/24; 2001:db8::/32; };
options {
  recursion yes;
  allow-qeury { my-net; };
};
```

There should not be issues

- Usually users automatically get DNS setting
  - PPPoE
  - DHCP
- System integrators who are responsible for enterprise network keep its setting up-to-date

real situations ☹

- Users statically setup DNS setting on their devices, and don’t change it forever even after switching ISPs
- Lazy system integrators uses nameservers which they just know and leave them forever
- Users change DNS setting based on a rumor that you can get more internet speed by changing DNS setting

One ISP tried in 2003

- Unexpected complaints
  - An enterprise used to be a customer of the ISP, claims they couldn’t access the internet
  - Business collaborators were using the ISP’s nameservers
- An executive of the ISP decided to stop the implementing BCP140 at that time

The ISP started to try it again in 2008

- Executives got involved
- Announcement based on query log
- Checking other ISP’s setting manuals
  - actually they found their nameserver there
- Introducing a phased restriction
  - Regional only -> Japan only -> their customer only

- They have done 98% in 2011, and still continuing

IIJ case

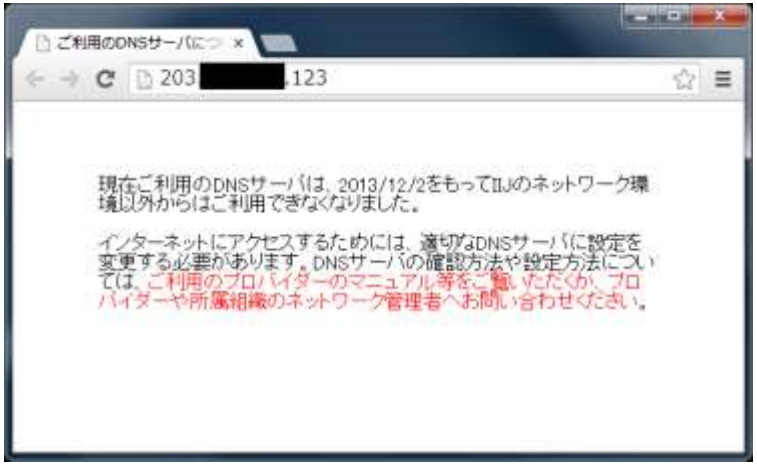
- public announcement on Sept 2013
  - “for those who used IIJ services before”
  - corporate web site
    - http://www.iij.ad.jp/company/development/tech/activities/open_resolver/
  - technical blog
    - http://techlog.iij.ad.jp/archives/718
  - news site
- about 3months before implementing

2st Dec 2013 12:00JST

- IIJ’s cache nameservers started to serve its customers only
- For queries from outside, the nameservers are answering static A to lead users to a warning web page.
  - saying “your dns setting is not valid anymore, so you need change your setting to access the internet. please contact your ISP or network administrator for further assistance.”

the warning page

- Simple text only
  - no javascript
  - no image
  - no link



203[redacted].123

現在ご利用のDNSサーバは、2013/12/2をもってIIJのネットワーク環境以外からはご利用できなくなりました。

インターネットにアクセスするためには、適切なDNSサーバに設定を変更する必要があります。DNSサーバの確認方法や設定方法については、ご利用のプロバイダーのマニュアル等をご覧いただくか、プロバイダーや所属組織のネットワーク管理者へお問い合わせください。

- At first we put the name of IIJ at the bottom, then users called IIJ by searching telephone number somehow
- So IIJ deleted its name, and emphasized “contact your ISP or network administrator”

Users

- Some users still could post messages on social medias - probably by using their smartphone
- Some of them were suggesting to use other publically available nameservers
  - google's
  - just usable ones ☹

collaboration with other ISPs

- Implementing BCP140 might increase # of customer calls at other ISPs' helpdesk
- ISPs announce schedule of the change to other ISPs in advance so that we can expect customer calls
- ISP community could develop a shared warning page that shows the right contact based on the source IP address of the client

lesson learned

- executive's approval to deal with complaint
- effective announcement
  - public and also targeted based on query log
- collaborating with other ISPs
  - for better customer support
- phased implementation could be your choice
- start early before the issue is getting bigger
  - more unexpected users will use the server

END