Open DNS Resolver Check Site

Hiroshi KOBAYASHI, Takayuki UCHIYAMA
Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Agenda

- Background
  - History

- Mechanism
  - Work Diagram
  - Countermeasure

- Statistics
  - Access History

- Collaboration
  - Domestic
  - International

Hiroshi KOBYASHI

koba is an Information Security Analyst at JPCERT Coordination Center, National CSIRT in Japan. He is in charge of incident response.

Takayuki UCHIYAMA

Taki is an Information Security Analyst at JPCERT Coordination Center, National CSIRT in Japan. He is in charge of handling vulnerability reports.
Open DNS Resolver Issue

- Open DNS resolver issue has been a persistent issue for quite a long period of time.
  - It was a big topic around 2006

- The number of open resolver hosts (since 2006) is shown at The Measurement Factory website.

Data source: The Measurement Factory
DNS Amplification Attack

Target (Victim)

192.0.2.123

Attacker

Source Address Spoofing
(192.0.2.123)

Very High Amplification

Open DNS Servers

Copyright © 2014 JPCERT/CC All rights reserved.
Open Resolver Issue in 2013

■ Spamhaus
— From 19/Mar/2013
— Over 300Gbps during 1 week span!
— Reported by CloudFlare

■ JPCERT/CC continues to receive many incident reports.

■ Small-scale DNS attacks are observed regularly in Japan.
Motivation for the check site

- Responsibility to protect our constituents!
- JPCERT/CC Initial Actions
  - Notification
    - Sent notifications to the appropriate contacts of Open Resolver hosts
  - Types of organizations / service providers contacted
    - User hosts on the hosting service
    - User hosts on the home
    - DNS servers on the enterprise environment
    - ISP DNS cache servers
Motivation for the check site

- Open Resolver hosts on the hosting service
  - Hosts often do NOT NEED to run a DNS server.
- Many host administrators are not aware of running DNS service on their own hosts.
  - Default Packages
    - OS image templates include DNS service as a server.
    - Software packages are delivered with Management Software that include DNS server components.
- Contacted individuals may be inappropriate for handling such an issue
- It is hard to get a good contact that can properly address the issue
Motivation for the check site

openresolver.jp

— Contacted Organizations
  ■ User hosts on the hosting service
  ■ User hosts on the home, ISP

— It can be extremely difficult for administrators/users to recognize if their host server/device is an open resolver or not.

— There are many similar open resolver check sites, but our site offers:
  ■ An easy and simple method
  ■ Increased awareness towards the open resolver issue to users that visit the site.
Open Resolver check site has been released

http://www.openresolver.jp/

JPCERT/CC では、オープンリゾルバとなっている DNS サーバが日本国内に多く存在していることを確認しています。また独自の調査を行っている Open Resolver Project によると、世界全体で約 2800万台（2013/10末現在）のオープンリゾルバが存在すると報告されています。

オープンリゾルバとは、外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS サーバのことです。オープンリゾルバは、個別に多数存在し、大規模な DDoS 攻撃の替玉として使用されているとの報告があります。

また、DNS サーバとして運用しているホストだけではなく、ブロードバンドルータなどのネットワーク機器が意図せずオープンリゾルバになっている事例があることを確認しています。

本確認サイトでは、お使いの PC に設定されている DNS サーバと、本確認サイトへの接続元となっているブロードバンドルータなどのネットワーク機器がオープンリゾルバとなっているかを確認することが可能です。

本サイトを活用し、健全なインターネット運用にご協力いただけますようお願いいたします。

| ホスティングサービスで使用しているサーバがユーザの意図しないままオープンリゾルバとなっている事例も多く報告されています。これらのホスト管理者の方が wget コマンドなどを使用してコマンドラインから確認できるサイトも用意しています。 |
| コマンドラインからの確認方法 |

※ 本サイトの公開時から2013年10月31日14時58分の間において、オープンリゾルバの可能性がある場合に表示される「設定されている DNS サーバ」と「接続元 IP アドレス」の IP アドレスの結果に誤りがありました。誤を訂正していただくようお願いいたします。

★ 本サイトの詳細については こちら をご参照ください。
Open DNS Resolver Check Site


JPCERT/CC has been observing situations where open DNS resolvers are spread widely across Japan. Moreover, according to the survey conducted by the Open Resolver Project, there exist about 28 million open DNS resolvers throughout the world (as of Oct 2013).

An open DNS resolver is a publicly accessible name server that provides a recursive name resolution for unspecified IP addresses. It has been reported that a number of open DNS resolvers are being exploited to participate in massive distributed denial of service (DDoS) attacks.

JPCERT/CC has also been observing situations where not only host computers that operate as DNS servers but also network devices (e.g. broadband routers) unintentionally running open DNS resolvers.

This site allows you to check on the following 2 points:
- Whether the DNS server configured on your PC is running an open DNS resolver or not
- Whether your network device (e.g. broadband router) connecting to this site is running an open DNS resolver or not

JPCERT/CC appreciates your contribution towards a robust cyber space by utilizing this check site.

JPCERT/CC has also received a number of reports where servers of hosting services are operating as open DNS resolvers, despite users' intentions. We have also set up another site for such host administrators to check their computers using command lines (e.g. "wget" command).

Try check site using command lines at the following URL:
http://www.openresolver.jp/di/check.html

The number of Open Resolvers in the world

![Chart showing the number of open resolvers, with data for outside Japan and Japan separately.](chart.png)
**Command line tool is also available**

For those that cannot check using a web browser, we have prepared a command based tool:

**wget:**

```
```

Configured DNS server: [OPEN] 192.0.2.2(ns.example.com)
Source IP address: [NOT open] 192.0.2.1(gw.example.com)

**curl:**

```
$ curl --location-trusted http://www.openresolver.jp/cli/check.html
```

Configured DNS server: [OPEN] 192.0.2.2(ns.example.com)
Source IP address: [NOT open] 192.0.2.1(gw.example.com)
The Measurement Factory Statistics

These graphs are also available at openresolver.jp

Data source: The Measurement Factory
How openresolver.jp Works

example

DNS Cache / Resolver
ISP
DNS server

Home Router
Local DNS Cache / Resolver

source IP address (home router)

DNS Server
Authority zone: openresolver.jp

www.openresolver.jp
How openresolver.jp Works

- Click “Submit” on the Agreement page

![Diagram showing the process]

- ISP DNS server
- Source IP address (home router)
- Generate One time unique URL
  
  "(random).chk.openresolver.jp"

- Web access (click submit button)
  
  www.openresolver.jp

- "0123xxxxxxxxxxxxxxxxxxxxxxxxx
cdef.0123xxxxxxxxxxxxxxxxxxxx
xxxxxcdef.chk.openresolver.jp"
How openresolver.jp Works

- Obtain IP address of ISP DNS server

DNS Server
Send a query
“(random).chk.openresolver.jp”

ISP
DNS server

resolve host name
(random).chk.openresolver.jp

Home Router
Send a query
“(random).chk.openresolver.jp”

source IP address
(home router)

www.openresolver.jp
How openresolver.jp Works

Send a DNS query (check.openresolver.jp) to each IP address → this step checks if it is an open resolver or not

ISP DNS server

source IP address (home router)

resolve host name check.openresolver.jp

www.openresolver.jp

cache a result for 1 hour
How openresolver.jp Works

- Obtain source IP address

Source IP address
(source IP address)
ISP
DNS server

Web access (result page)

Configured DNS server: Not an open DNS resolver. Source IP address: Not an open DNS resolver.

Source IP address (home router)

www.openresolver.jp
Sample result page

Configured DNS server: Not an open DNS resolver.
Source IP address: Not an open DNS resolver.

Configured DNS server: Possibly an open DNS resolver.
Source IP address: Not an open DNS resolver.
Instruction for openresolver users

- Visitors can also follow the instructions to address the issue
- Countermeasure process
  — Configure DNS appropriately
  — Send the check results to JPCERT/CC
- Home Router brand name, version and etc.
- Useful links on additional technical information
Openresolver.jp Statistics

Statistics

— Site Access to www.openresolver.jp

Source device (Home Router)

- source IP address

<table>
<thead>
<tr>
<th>Year</th>
<th>NOT Open resolver</th>
<th>Open resolver</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013/10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2013/11</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>2013/12</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>2014/01</td>
<td>825</td>
<td>825</td>
</tr>
<tr>
<td>2014/02</td>
<td>13,500</td>
<td>13,500</td>
</tr>
<tr>
<td>2014/03</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2014/04</td>
<td>10,000</td>
<td>10,000</td>
</tr>
<tr>
<td>2014/05</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Graph showing number of accesses (unique IP address) over time.
Openresolver.jp Statistics

Statistics

—Site Access to www.openresolver.jp

ISP DNS Server

ISP DNS Server

<table>
<thead>
<tr>
<th>Month</th>
<th>NOT Open Resolver</th>
<th>Open Resolver</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013/10</td>
<td>400</td>
<td>100</td>
</tr>
<tr>
<td>2013/11</td>
<td>400</td>
<td>100</td>
</tr>
<tr>
<td>2013/12</td>
<td>400</td>
<td>100</td>
</tr>
<tr>
<td>2014/01</td>
<td>1200</td>
<td>200</td>
</tr>
<tr>
<td>2014/02</td>
<td>1200</td>
<td>200</td>
</tr>
<tr>
<td>2014/03</td>
<td>1200</td>
<td>200</td>
</tr>
<tr>
<td>2014/04</td>
<td>1200</td>
<td>200</td>
</tr>
<tr>
<td>2014/05</td>
<td>1200</td>
<td>200</td>
</tr>
</tbody>
</table>

Copyright © 2014 JPCERT/CC All rights reserved.
Conclusion – Results obtained from the site

According to MF

— The number of Open Resolver hosts continues to decrease
— If this pace holds up, we have hope that this issue may be cleared up in 4 years

Of course, we would like it to be addressed sooner!

Data source: The Measurement Factory
In the future…

- Wishful thinking says that as use of our site increases (along with other available sites) the number of open resolvers will decrease
  - But in reality, just “using” the site will not decrease the number of open resolvers
  - Countermeasures need to be put in place to eliminate the open resolvers
  - In some cases coordination is necessary

- JPCERT/CC will continue its efforts to address this issue domestically and will collaborate with any global partners that need assistance with this issue
**Recent DDoS Trends**

- **Other UDP protocols other than DNS**
  - 123/ucp (ntp), 161/udp (snmp), 19/udp (chargen), 7/udp(echo)

![Graph showing recent DDoS trends with UDP protocol usage](Image)
Contact Information

General Contact
— Email: office@jpcert.or.jp
— Tel: +81.3.3518.4600
— https://www.jpcert.or.jp

Incident Reporting
— Email: info@jpcert.or.jp
— PGP Public Key: https://www.jpcert.or.jp/english/ir/pgp.html
— Incident Reporting Form: https://www.jpcert.or.jp/english/ir/form.html