Problems with Open DNS Resolver

- NOTICE **Starting on 2014/01/20 (A), an IP address will automatically be blocked if open DNS resolver is detected.** Users must correct the problem to avoid being blocked from the network. **See Abused Network Usage if you were blocked.**

Problem Overview

An Open DNS resolver is when the Caching recursive DNS server provides recursive name resolution service to the public (subjects not limited), which may cause the following problems:

1. Exposure to the outside world, making it is easy to be attacked or **lose system and network resources**.
2. Occurrence of **cache poison**.
3. **Easy to be used by the outside world and become a member of DDoS cyber attacks.**

Detection system

NEWWe developed an open DNS resolver detection system to prevent the open DNS resolver problem and help handle computers on campus with incorrect settings, so that they are not exploited by attackers to launch cyber attack. **Detection results are provided to network administrators of each unit, so that they may forward the information and suggested methods to users to correct settings, or inspect if the problem was solved**. We hope that this will reduce the number of computers with open DNS resolver on campus.

Real-time Detection Service

NEWWe developed this detection service to make it easier for NTHU users to detect whether their computers or network devices have an open DNS resolver. At present, **only NTHU IP addresses can use the detection service**. 2013/08/30 online trial)

Detect open DNS server IP address: 1 . 1 . . .   Start testing Clear

- NOTICEBefore performing the test, **please check if the computer or device at the target IP address is on and the network connection is normal**, so that the detection result is not affected.

Detection results

- A result similar to the one below indicates a problem with open DNS resolver.
  - **It should not reply to DNS inquiries not under its jurisdiction**

```
Check open dns resolver for the target IP 140.114.xx.xx
```

```
Time: Wed Sep 11 09:10:11 2013

check_open_resolver: 140.114.xx.xx
DIG:
DIG: ; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.xx.xx -t A isc.org
DIG: ; (1 server found)
DIG: ;; global options: +cmd
DIG: ;; Got answer:
DIG: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13648
DIG: ;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4,
ADDITIONAL: 2
DIG:
DIG: ;; QUESTION SECTION:
DIG: ;isc.org.          IN    A
DIG:
DIG: ;; ANSWER SECTION:
DIG: isc.org.       60    IN    A    149.20.64.69
DIG:
DIG: ;; AUTHORITY SECTION:
DIG: isc.org.       1814    IN    NS    sfba.sns-pb.isc.org.
DIG: isc.org.       1814    IN    NS    ns.isc.afilias-nst.info.
DIG: isc.org.       1814    IN    NS    ams.sns-pb.isc.org.
DIG: isc.org.       1814    IN    NS    ord.sns-pb.isc.org.
DIG:
DIG: ;; ADDITIONAL SECTION:
DIG: ns.isc.afilias-nst.info. 54300 IN    A    199.254.63.254
DIG: ns.isc.afilias-nst.info. 54300 IN    AAAA    2001:500:2c::254
DIG:
DIG: ;; Query time: 402 msec
DIG: ;; SERVER: 140.114.xx.xx#53(140.114.xx.xx)
DIG: ;; WHEN: Wed Sep 11 09:10:11 2013
DIG: ;; MSG SIZE  rcvd: 184
DIG:

CHECK : Is 140.114.xx.xx an open resolver?
ANSWER: YES for 140.114.xx.xx
REASON: IP 140.114.xx.xx should not reply the DNS request which
does not belong to its authorized zone.
```

- A result similar to the one below **indicates there is no problem with open DNS resolver**.
  1. **DNS can't be connected.**If the computer is on and the network is normal, there is no problem with this computer.

```
Check open dns resolver for the target IP 140.114.63.1
Time: Wed Sep 11 09:26:32 2013

check_open_resolver: 140.114.63.1
DIG:
DIG: ; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.63.1 -t A isc.org
DIG: ; (1 server found)
DIG: ;; global options: +cmd
```

```
DIG: ;; connection timed out; no servers could be reached

CHECK : Is 140.114.63.1 an open resolver?
ANSWER: NO for 140.114.63.1
REASON: Cannot reach 140.114.63.1. If its power is off, please
turn it on and check again.
```

2. **Reject recursive query**

```
Check open dns resolver for the target IP 140.114.63.10
Time: Wed Sep 11 09:27:47 2013

check_open_resolver: 140.114.63.10
DIG:
DIG: ; <<>> DiG 9.6-ESV-R7-P2 <<>> @140.114.63.10 -t A isc.org
DIG: ; (1 server found)
DIG: ;; global options: +cmd
DIG: ;; Got answer:
DIG: ;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 7118
DIG: ;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0
DIG: ;; WARNING: recursion requested but not available
DIG:
DIG: ;; QUESTION SECTION:
DIG: ;isc.org.          IN    A
DIG:
DIG: ;; Query time: 2 msec
DIG: ;; SERVER: 140.114.63.10#53(140.114.63.10)
DIG: ;; WHEN: Wed Sep 11 09:27:47 2013
DIG: ;; MSG SIZE  rcvd: 25
DIG:

CHECK : Is 140.114.63.10 an open resolver?
ANSWER: NO for 140.114.63.10
REASON: Recursion requested but not available
```

Suggested method

Windows 7

- Please select method A, B, or C below based on your own situation.

A. Disable Windows 7 (ICS) service to prevent DNS service

- Disable Windows 7 (ICS) service to prevent open DNS resolver

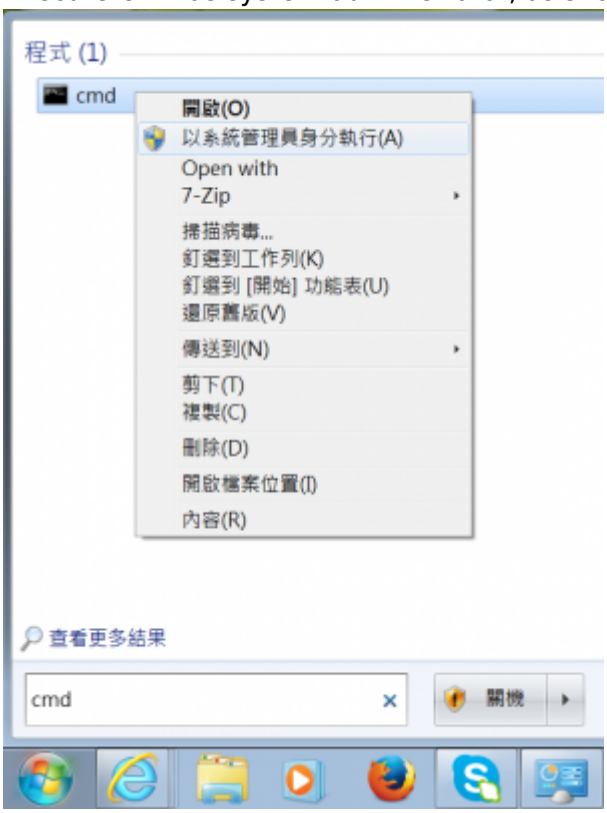
B. Use a firewall to block DNS service

- Use a firewall to **reject any DNS inquiry packets (UDP/53)**

1. Configure Windows 7 firewall to prevent open DNS resolver
2. Configure Symantec firewall to prevent open DNS resolver

C. Find the corresponding program of DNS service and close it

1. Execute CMD as system administrator, as shown in the figure below



2. Execute the **netstat -ab -p UDP** command. Using the box below as an example, find **UDP 0.0.0.0:53 (indicates that it provides DNS service)**, which corresponds to the component XXXXX and the program [yyyy.exe].

```
C:\Windows\system32>netstat -ab -p UDP

使用中連線

  協定    本機位址               外部位址               狀態
  UDP    0.0.0.0:500            *:*
  IKEEXT
 [svchost.exe]
...
  UDP    0.0.0.0:53             *:*
  XXXXX
 [yyyyy.exe]
...
```

   - For example, the figure below shows that the component SharedAccess and the program svchosts.exe is what causes open DNS resolver. Users should determine whether or not

the program and its settings can be terminated.