JPCERT-IA-2014-02

Issued: 2014-07-17

# JPCERT/CC Internet Threat Monitoring Report [April 1, 2014 - June30, 2014]

## 1 Overview

JPCERT/CC has placed multiple sensors across the Internet for monitoring to continuously gather packets which are dispatched to indefinite nodes on the Internet. These packets are categorized by the destination port number, source region, etc. Then this information is analyzed along with information about vulnerabilities, malware and attack tools to obtain information on attacking activities or preparatory activities. This report will mainly show the analysis results of packets targeted to Japan during this quarter.

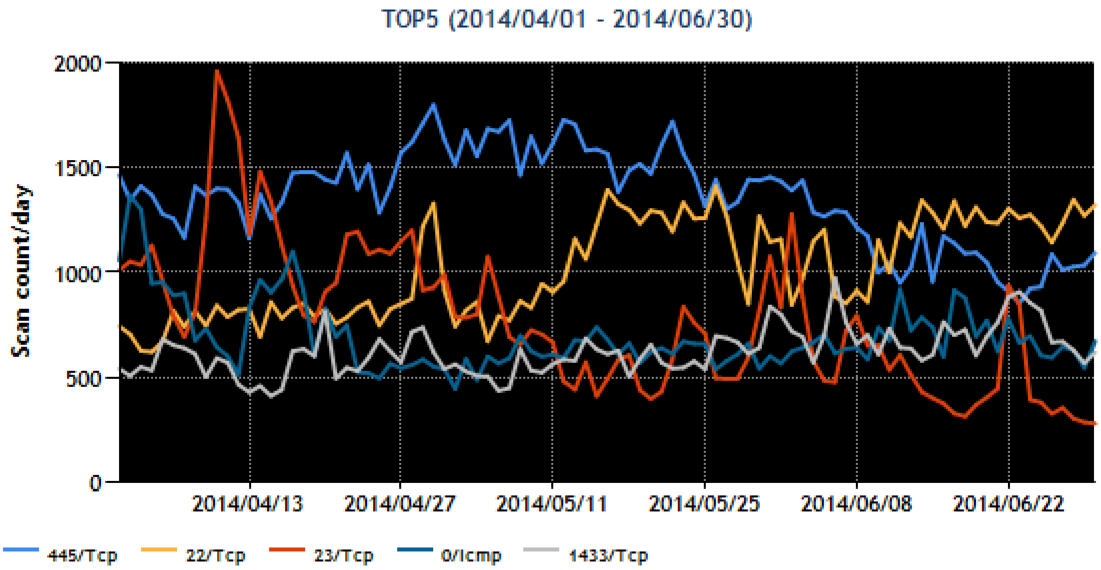
The top 5 destination port numbers for which packets were observed are listed in [Chart 1].

[Chart1: Top 5 destination port numbers]

| Destination Port Numbers | This Quarter | Previous Quarter |
|---|---|---|
| 445/TCP (microsoft-ds) | 1 | 1 |
| 22/TCP (ssh) | 2 | 3 |
| 23/TCP (telnet) | 3 | 2 |
| 0/ICMP | 4 | 4 |
| 1433/TCP (ms-sql-s) | 5 | 5 |

*For details on services provided on each port number, please refer to the documentation provided by IANA(*1). The service names listed are based on the information provided by IANA, but this does not always mean that the packets received are relevant for that service / protocol.

[Figure1] shows the change over the 3 month period in the number of packets that the top 5 destination ports received.



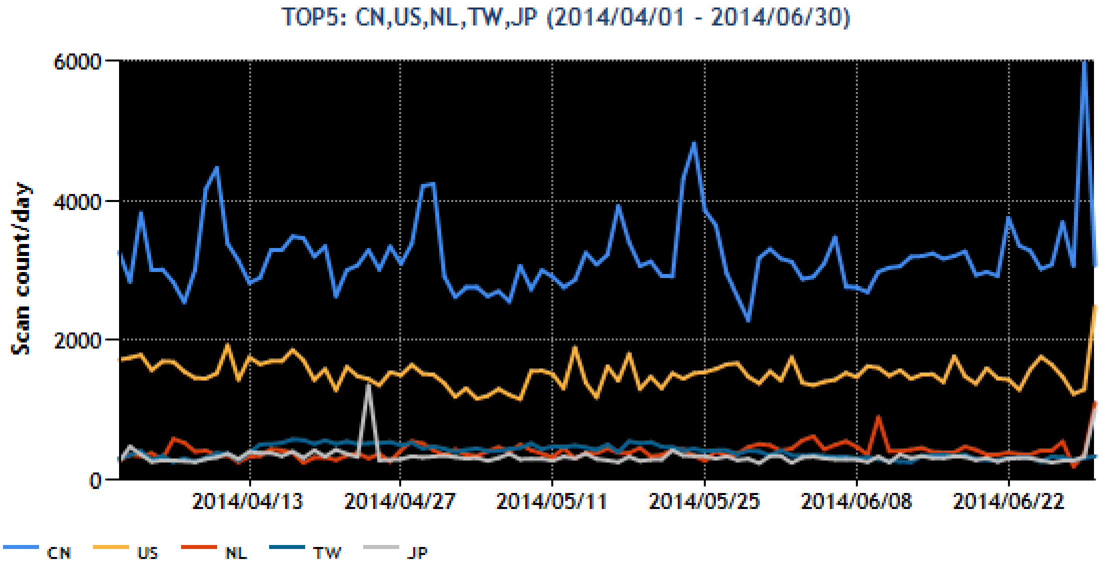
[Figure1: Number of packets observed at top 5 destination ports from April through June 2014]

The top 5 source regions of packets observed are listed in [Chart 2].

[Chart2: Top 5 source regions]

| Source Regions | This Quarter | Previous Quarter |
|---|---|---|
| China | 1 | 1 |
| USA | 2 | 2 |
| Netherlands | 3 | 4 |
| Taiwan | 4 | 6 |
| Japan | 5 | 3 |

[Figure2] shows the change over the 3 month period in the number of packets sent from the top 5 source regions.



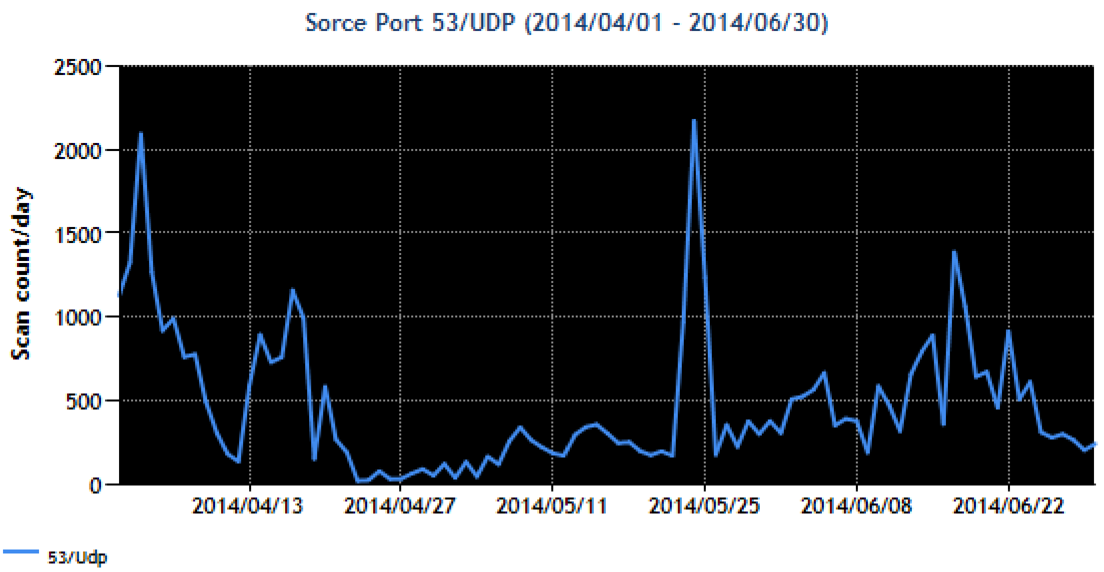
[Figure2: Number of packets observed from the top 5 source regions from April through June 2014]

During this quarter, there was a gradual increase in the number of packets targeted to 22/TCP. While 23/TCP fell to third place this quarter from the previous quarter(second place), it remains a popular target. There were some increases and decreases at other ports, but there was nothing of note.

## 2 Events of Note

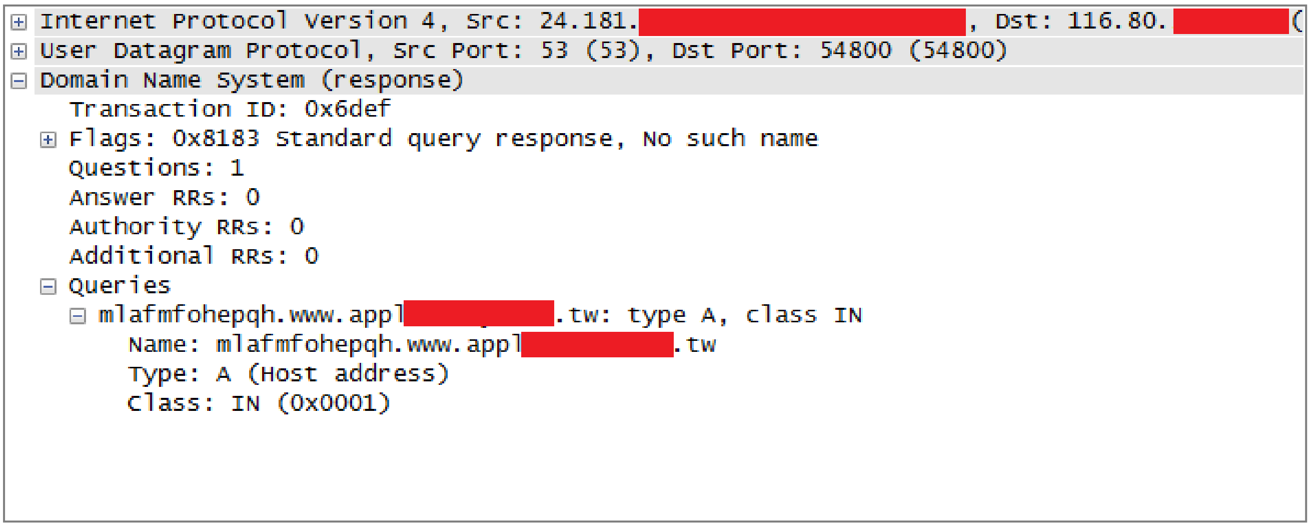
### 2.1 DNS answer packets and ICMP error packets indicating that DNS service port was unreachable have been observed

A large number of packets using source port number 53/UDP (herein, "DNS answer packets") and ICMP error packets indicating that the destination DNS service port was unreachable continued to be observed during this quarter.



[Figure3: Number of packets observed with source port number 53/UDP from April through June 2014]

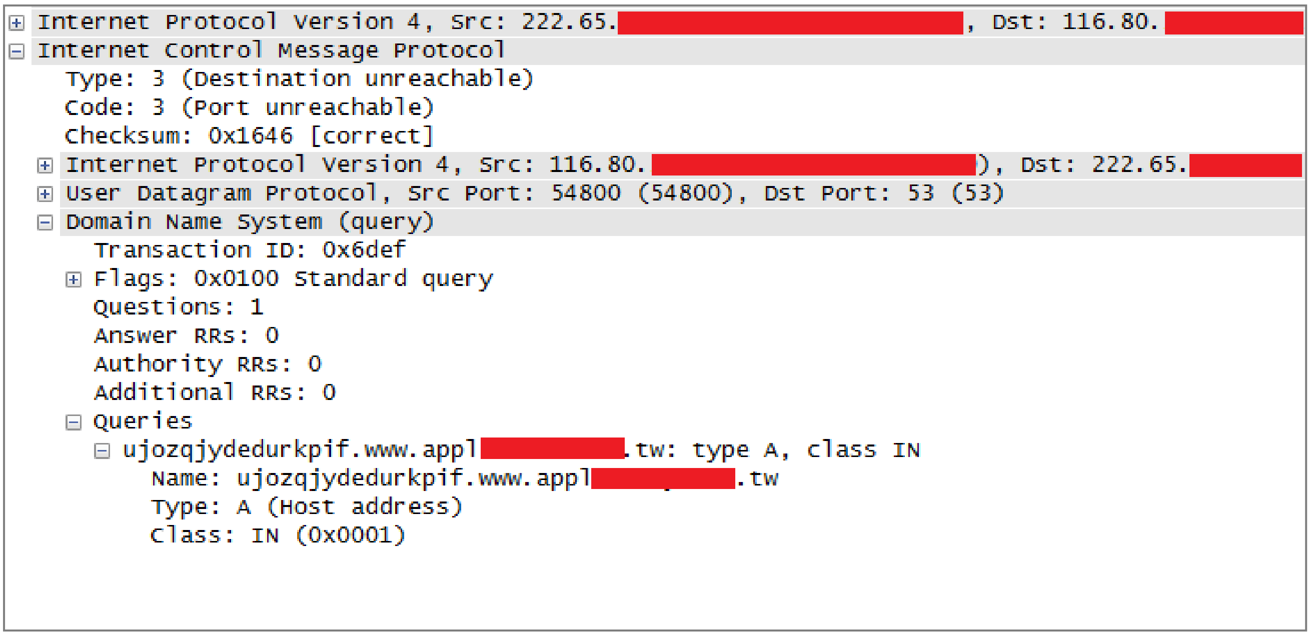
JPCERT/CC has analyzed the DNS answer packets received by one of the sensors, and found that they were responses to queries of nonexistent FQDNs (containing strings of random characters), as shown in Figure4.



```
⊞ Internet Protocol Version 4, Src: 24.181.[redacted], Dst: 116.80.[redacted](
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 54800 (54800)
⊟ Domain Name System (response)
    Transaction ID: 0x6def
  ⊞ Flags: 0x8183 Standard query response, No such name
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ mlafmfohepqh.www.appl[redacted].tw: type A, class IN
        Name: mlafmfohepqh.www.appl[redacted].tw
        Type: A (Host address)
        Class: IN (0x0001)
```

[Figure4: Packet with source port number 53/UDP captured in June 2014 (displayed with Wireshark)]

These DNS answer packets were transmitted in response to DNS query packets sent by an attacker. The attacker was attempting to flood the targeted authoritative DNS servers by sending queries of a large number of nonexistent FQDNs via cache DNS servers that allow recursive queries from unspecified hosts (via the Internet), or devices that transfer DNS queries (via DNS forwarding) from unspecified hosts to the cache DNS servers provided by ISPs, etc. (herein collectively, "open resolvers"). It is presumed that the packets were received by the sensor because the fraudulent source IP address used by the attacker happened to be identical to the IP address allocated to the sensor. In other words, the sensor observed repercussions of a DDoS attack targeting authoritative DNS servers.



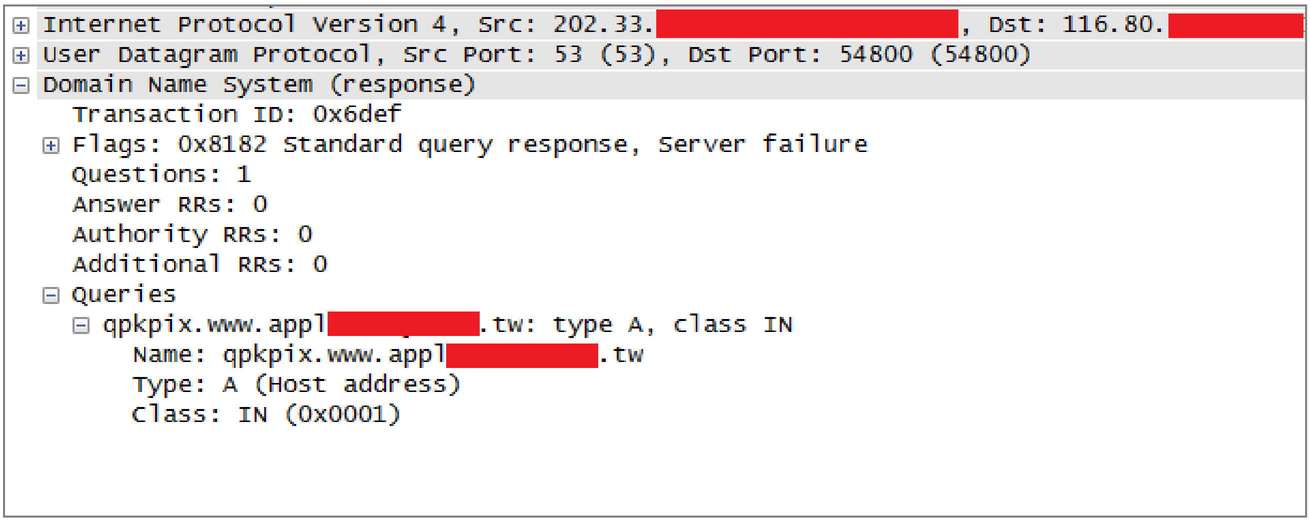
```
⊞ Internet Protocol Version 4, Src: 222.65.[redacted], Dst: 116.80.[redacted]
⊟ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x1646 [correct]
  ⊞ Internet Protocol Version 4, Src: 116.80.[redacted]), Dst: 222.65.[redacted]
  ⊞ User Datagram Protocol, Src Port: 54800 (54800), Dst Port: 53 (53)
  ⊟ Domain Name System (query)
      Transaction ID: 0x6def
    ⊞ Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    ⊟ Queries
      ⊟ ujozqjydedurkpif.www.appl[redacted].tw: type A, class IN
          Name: ujozqjydedurkpif.www.appl[redacted].tw
          Type: A (Host address)
          Class: IN (0x0001)
```

[Figure5: ICMP error against source port number 53/UDP captured in June 2014 (displayed with Wireshark)]

Meanwhile, ICMP error packets (Figure5) indicating that the destination DNS service port number was unreachable appear to have reached the sensors because some of the nodes that were intended to be used for the abovementioned attack were no longer open resolvers, preventing the attack packets from going through.

The authoritative DNS servers that appear to have been the target of the DDoS attack were for a number of overseas domains that included a news site, an Internet voting site and a Contents Delivery Network (CDN). So far, there are no confirmed cases in which a domestic domain has become the target of attack. However, this attack has abused a large number of open resolvers in Japan, and the fact that these open resolvers have become party to the attack, even if unwittingly, is a serious problem.

In addition, open resolvers that participate in an attack end up surging the load on not only the targeted authoritative DNS servers, but also cache DNS servers provided by ISPs, etc., placed between the open resolvers and authoritative DNS servers. This can result in errors like the one shown in Figure6 (Server failure) getting returned in response to queries from clients using the same cache DNS server, thereby preventing such activities as web browsing and transmission of e-mail.



```
⊞ Internet Protocol Version 4, Src: 202.33.[redacted], Dst: 116.80.[redacted]
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 54800 (54800)
⊟ Domain Name System (response)
    Transaction ID: 0x6def
  ⊞ Flags: 0x8182 Standard query response, Server failure
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ qpkpix.www.appl[redacted].tw: type A, class IN
        Name: qpkpix.www.appl[redacted].tw
        Type: A (Host address)
        Class: IN (0x0001)
```

[Figure6: Packet with source port number 53/UDP captured in June 2014 (displayed with Wireshark)]

In order to reduce the number of open resolvers that are being used as springboards for attacks like the one mentioned above, please pay attention to the following points in particular.

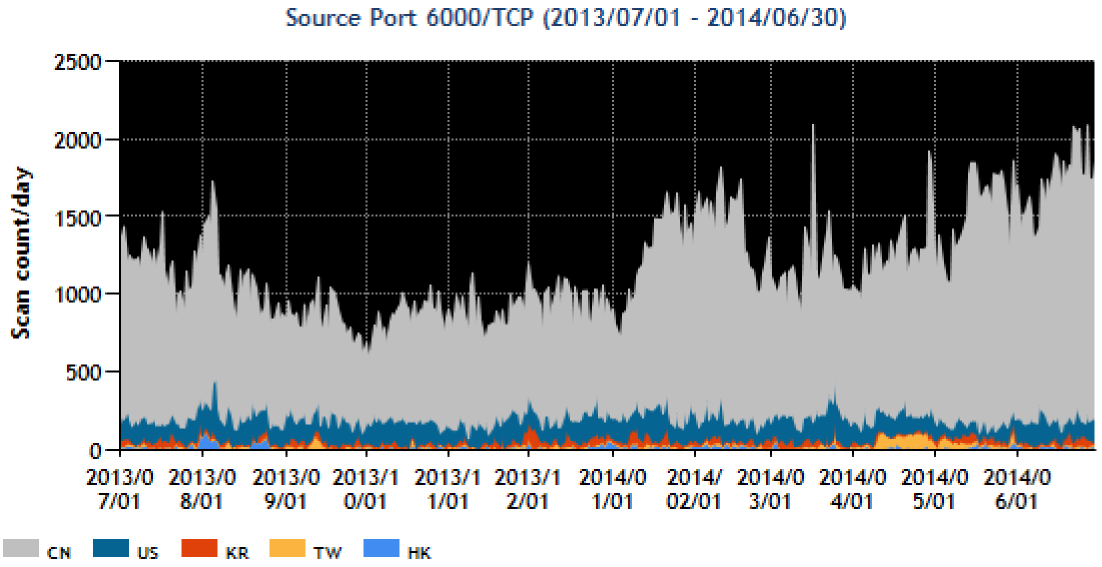
1. If DNS servers are used, please review the settings, such as the range of recursive queries that are accepted, and restrict access to the minimum necessary extent. (*2, 3, 4)

2. If gateway routers facing the Internet or other network devices equipped with DNS server or DNS forwarder functionality are used, please ensure that the settings are configured so as not to respond to DNS queries from an unspecified host. It is recommended that the settings are verified using the information published by each product vendor as a reference. (*4, 5)

3. If public servers such as a web server are being operated, make sure that no unnecessary DNS server is in operation.

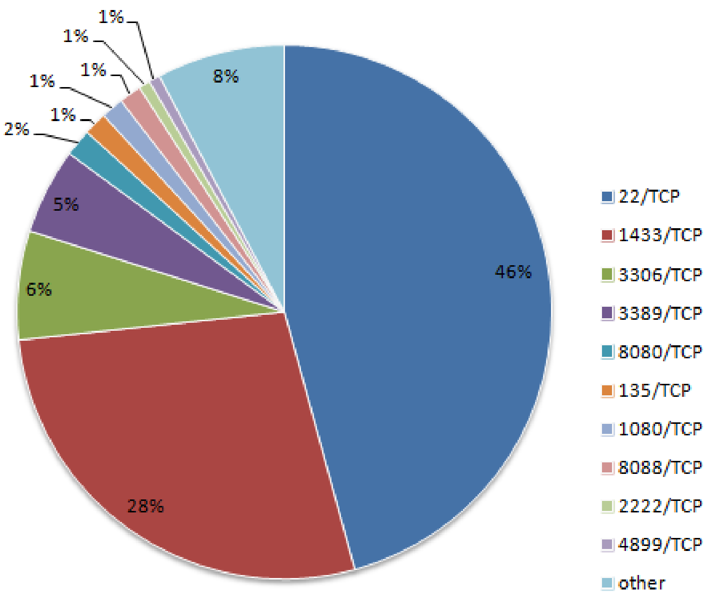
### 2.2 Packets with source port number 6000/TCP

The number of packets with source port number 6000/TCP has been on the rise since around the 4th quarter of FY 2013 (January 2014). These packets make up the largest proportion−approximately 20%−of all the packets targeted to Japan this quarter, and many of them originate from China.



[Figure7: Number of packets observed with source port number 6000/TCP from July 2013 through June 2014]

Many of these packets with source port number 6000/TCP are related to attacking activities or preparatory activities. Figure8 gives a breakdown of the destination ports of packets with source port number 6000/TCP for this quarter.



[Figure8: Composition of destination ports with source port number 6000/TCP from April through June 2014]

[Table3: Top 10 destination ports of packets with source port number 6000/TCP]

| This Quarter | Destination Port Numbers |
|---|---|
| 1 | 22/TCP (ssh) |
| 2 | 1433/TCP (ms-sql-s) |
| 3 | 3306/TCP(mysql) |
| 4 | 3389/TCP(ms-wbt-server) |
| 5 | 8080/TCP (http-alt) |
| 6 | 135/TCP (epmap) |
| 7 | 1080/TCP (socks) |
| 8 | 8088/TCP (radan-http) |
| 9 | 2222/TCP (EtherNet-IP-1) |
| 10 | 4899/TCP (radmin-port) |

*For details on services provided on each port number, please refer to the documentation provided by IANA(*1). The service names listed are based on the information provided by IANA, but this does not always mean that the packets received are relevant for that service / protocol.

JPCERT/CC has analyzed these packets with source port number 6000/TCP, and found that they were being sent from the same source IP address to a specific destination IP address on a regular basis (one packet once every few days), and that the window size was fixed to a specific values. These observations point to the likelihood that they are part of reconnaissance activities using a specific foreign-made tool. (*6, 7)

## 3 References

(1) Service Name and Transport Protocol Port Number Registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2) Japan Registry Services Co., Ltd. (JPRS)
Open resolvers: Inappropriate settings of DNS servers <Japanese only>
http://jprs.jp/important/2013/130418.html

(3) Japan Network Information Center (JPNIC)
Note on open resolvers <Japanese only>
https://www.nic.ad.jp/ja/dns/openresolver/

(4) JPCERT/CC
Open resolver verification site <Japanese only>
http://www.openresolver.jp/

(5) JVN#62507275 A number of broadband routers known to function as open resolvers <Japanese only>
https://jvn.jp/jp/JVN62507275/

(6) National Police Agency @Police
Information Technology Analysis 2013 Annual Report Annex "Internet Observation Results" <Japanese only>
http://www.npa.go.jp/cyberpolice/detect/pdf/H25_betsu.pdf

(7) National Police Agency @Police
Internet Observation Results (November 2013) <Japanese only>
http://www.npa.go.jp/cyberpolice/detect/pdf/20140206_2.pdf

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Coordination Activities for International Cooperation in Responding to Cyber Attacks for the 2014

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (office@jpcert.or.jp).

For the latest information, please refer to JPCERT/CC's website.

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/tsubame/report/index.html