

Report from the Internet Monitoring (TALOT2)

June 2009

1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in June totaled **115,860** cases for the 10 monitoring points and the gross number of the sources* was **41,065**: unwanted (one-sided) access captured at one monitoring point was about **386** accesses from about **137** sources per day (see the Chart 1-1).

Gross Number of Source (*): The gross number of the source accessed TALOT2. For your further information, the source is counted as 1 when accessed by the same source from the same day to the same point/port.

The environment for each monitoring point in TALOT2 is nearly equal to general users' Internet connection; it can be considered that the same amount of unwanted (one-sided) access may be received by the general internet users.

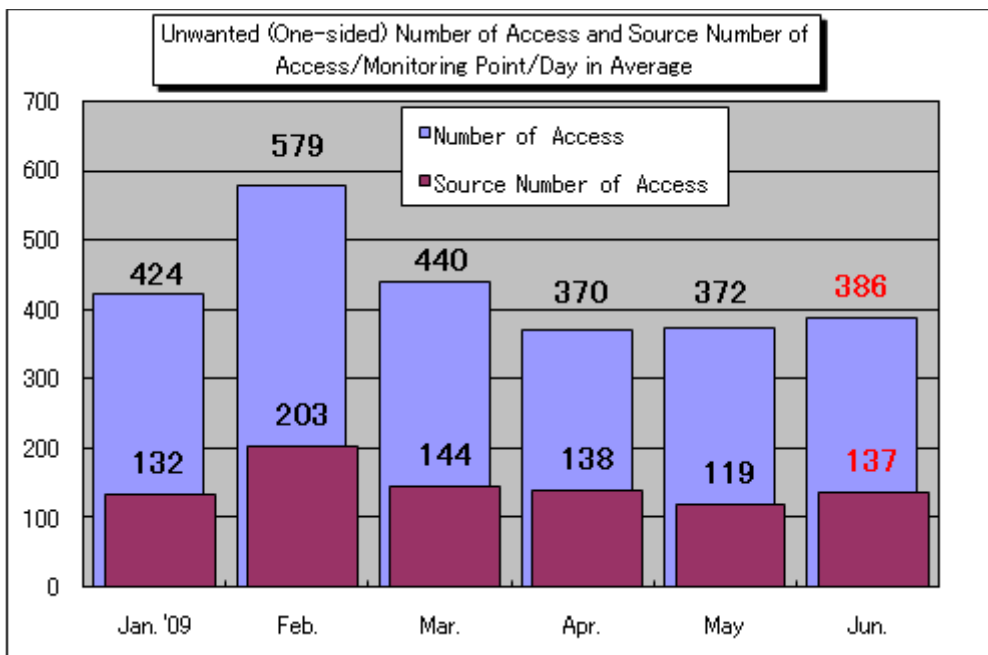


Chart 1-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day

The chart 1-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day in average from January to June 2009. Both the unwanted (one-sided) number of accesses were subtly increased compared with the ones in May.

The Chart 1-2 shows the comparison in both number of access classified by destination (by port) for the months of May and June.

In June, the number of access to the port 445/tcp was significantly increased compared with the one in May since the access to that port from overseas was increased (See the Chart 1-3).

The cause why such access from overseas was increased has not yet identified; however, the number of access from specific source was not increased, but the entire source number of access from overseas itself was directly relevant to that increase.

In addition, we'd obtained such information that the access to the port 445/tcp from overseas was increased from the other organization who also conducts the Internet monitoring.

As for the other ports other than the port 445/tcp were not significantly shifted, but the accesses to the ports other than the worst 10 ports were significantly decreased.

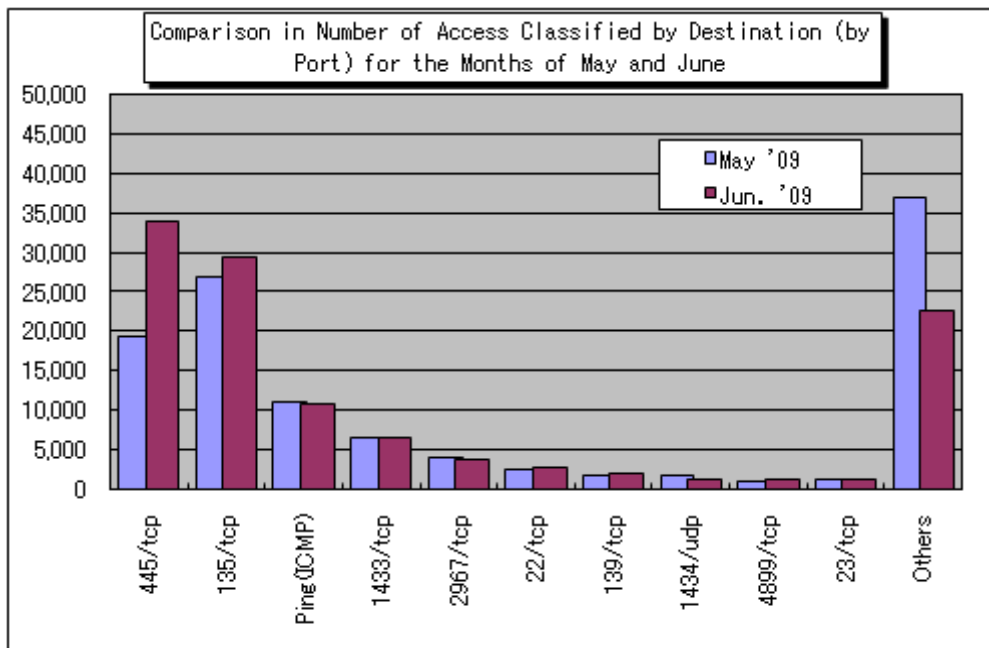


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) for the Months of May and June

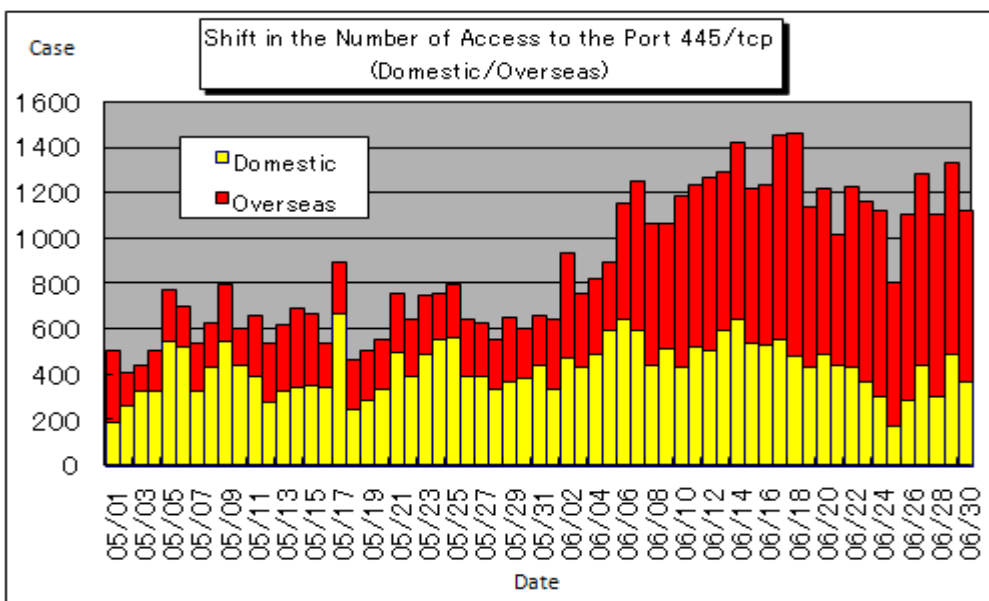


Chart 1-3: Number of Access to the Port 445/tcp (Domestic/Overseas)

2. The One-sided Accessing Status in June 2009

(1) Accessing Status Classified by Destination (by Port)

The Chart 2-1 shows the shift in unwanted (one-sided) accessing status (number of access) and the Chart 2-2 shows the shift in unwanted (one-sided) accessing status (source number of access) in June 2009.

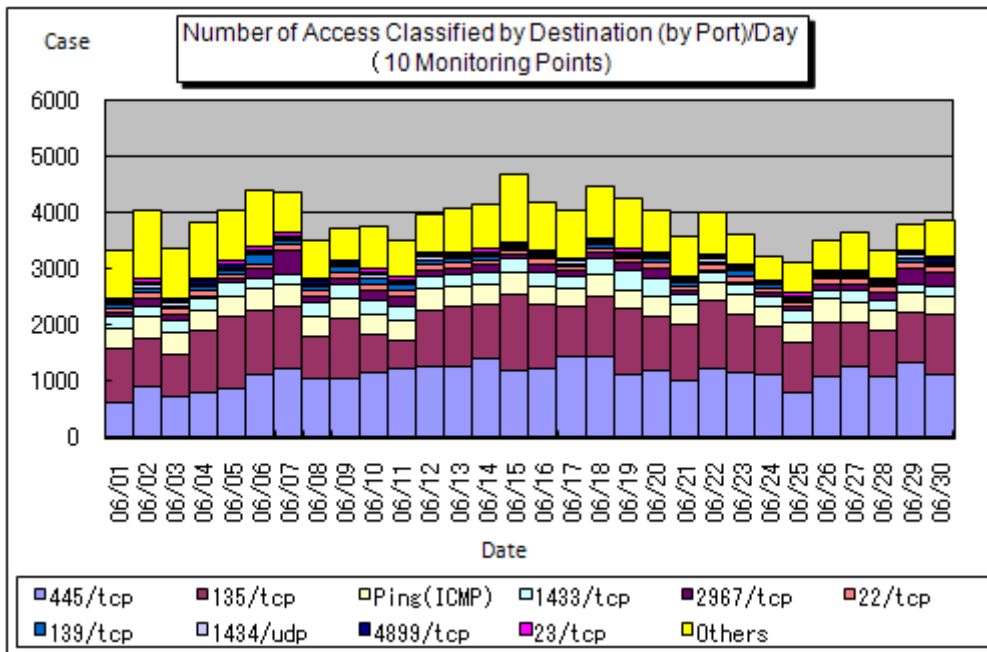


Chart 2-1: Number of Access Classified by Destination (by Port)/Day in June (10 Monitoring Points)

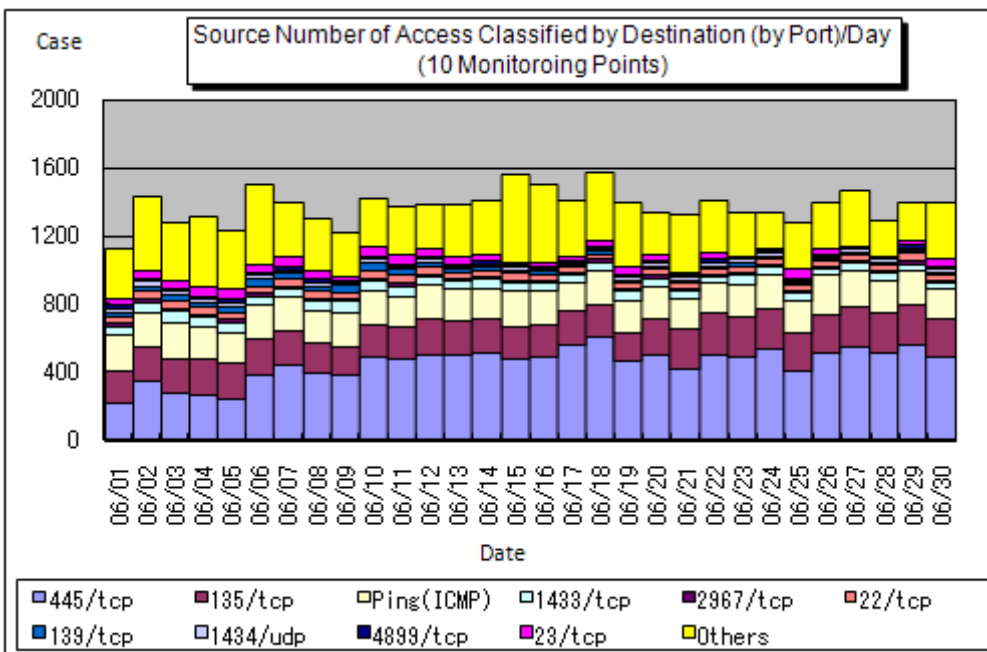


Chart 2-2: Source Number of Access Classified by Destination (by Port)/Day in June (10 Monitoring Points)

(2) Ratio Classified by Destination (by Port)

The Chart 2-3 shows the ratio in number of access classified by destination (by port) and the Chart 2-4 shows the ratio in source number of access classified by destination (by port) in June 2009. For your further information, each ratio is rounded at the 1st arithmetic point so that they may not make 100% sharp, accordingly.

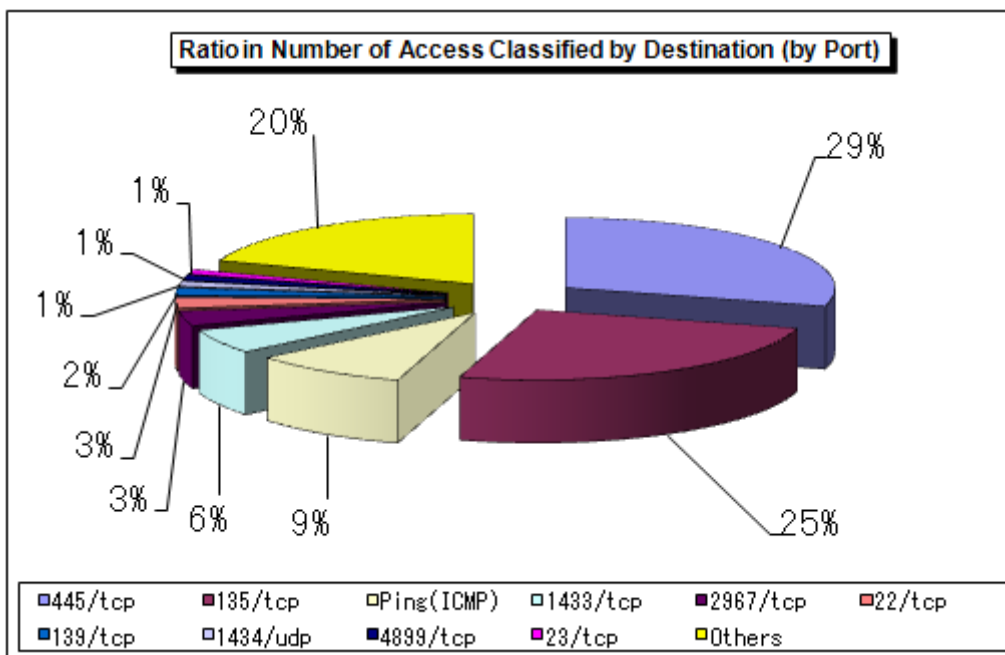


Chart 2-3: Ratio in Number of Access Classified by Destination (by Port) in June 2009

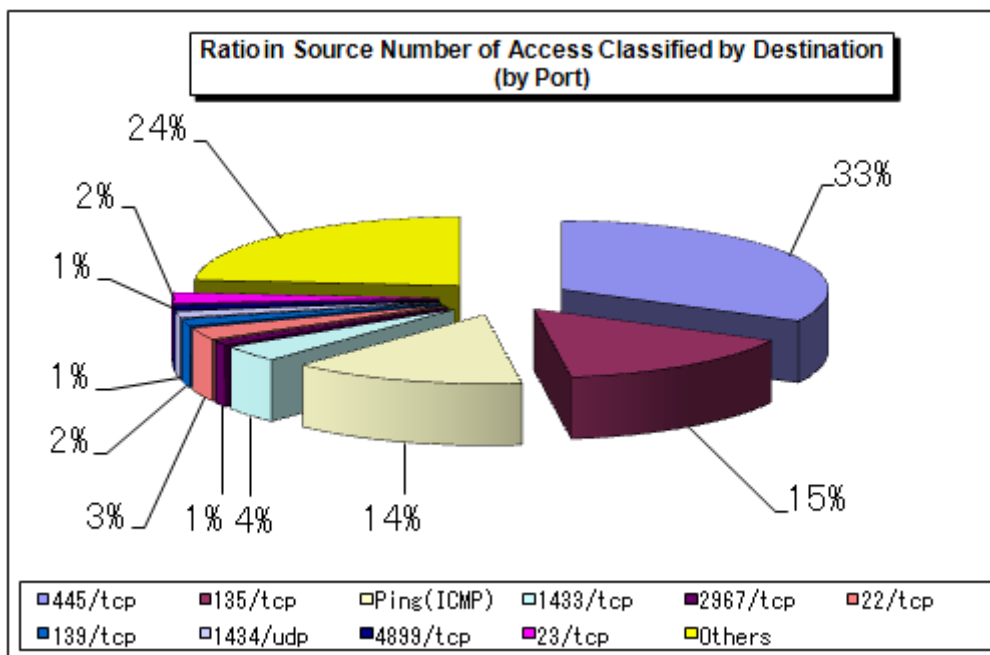


Chart 2-4: Ratio in Source Number of Access Classified by Destination (by Port) in June 2009

(3) Accessing Status Classified by Source Area

The Chart 2-5 shows the shift in number of access classified by number of access classified by unwanted (one-sided) source area and the Chart 2-6 shows the ratio in number of access classified by source area in June 2009. For your further information, each ratio is rounded at the 1st arithmetic point so that they may not make 100% sharp, accordingly.

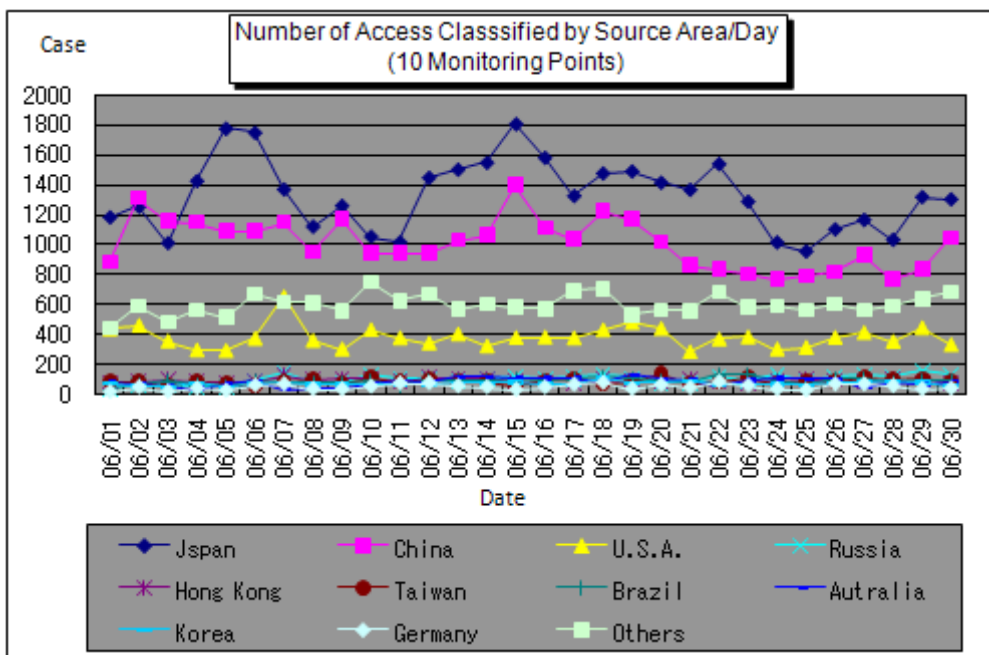


Chart 2-5: Number of Access Classified by Source Area/Day in June (10 Monitoring Points)

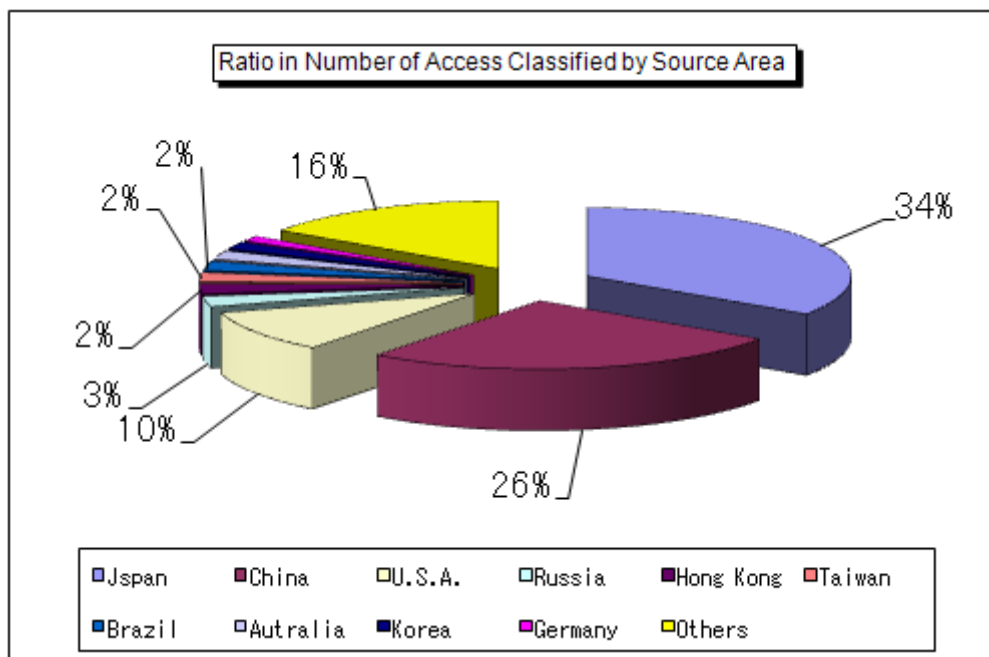


Chart 2-6: Ratio in Number of Access Classified by Source Area in June 2009

The Chart 2-7 shows the shift in source number of access classified by source area and the Chart 2-8 shows the ratio in source number of access classified by source area in June 2009. For your further information, each ratio is rounded at the 1st arithmetic point so that they may not 100% sharp, accordingly.

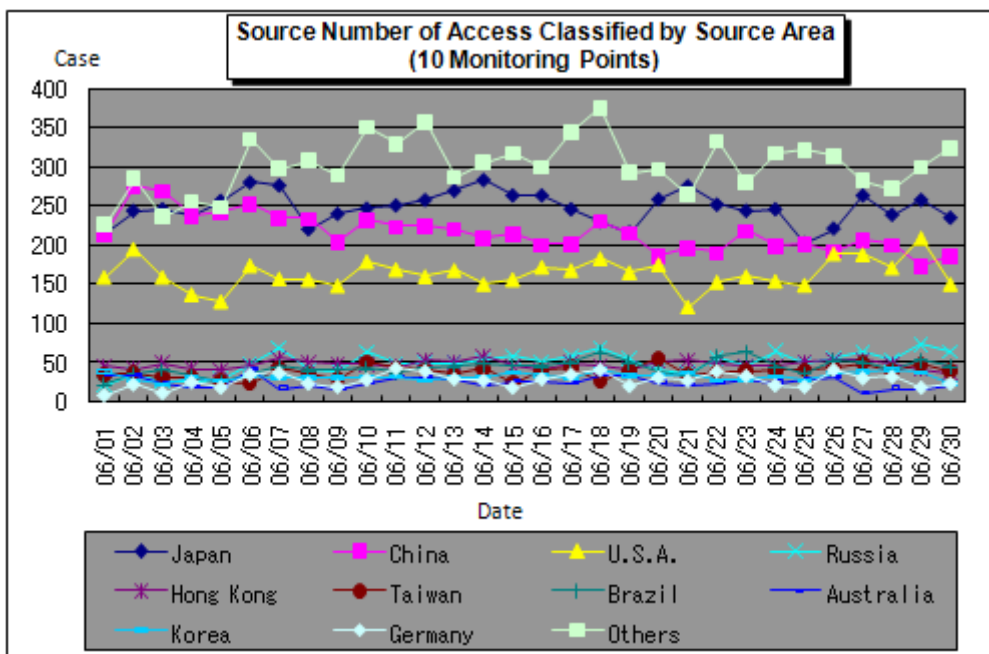


Chart 2-7: Source Number of Access Classified by Source Area/Day in June (10 Monitoring Points)

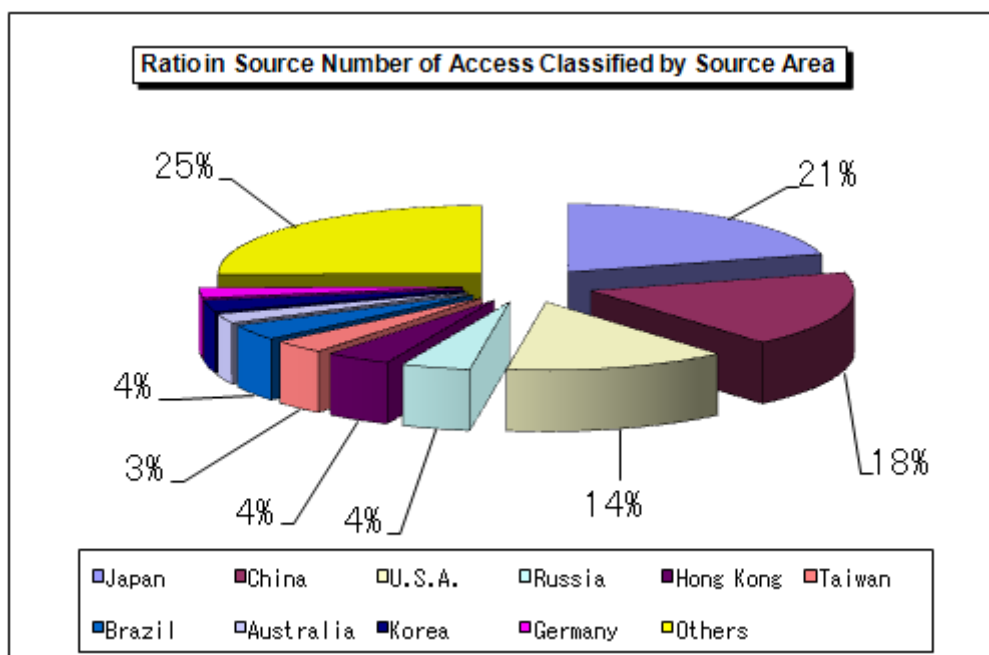


Chart 2-8: Ratio in Source Number of Access Classified by Source Area in June 2009

3. Statistical Information

(1)Ratio Classified by Destination (by Port)

The Chart 3-1 shows the ratio in number of access classified by destination (by port) and the Chart 3-2 shows the ratio in source number of access classified by destination (by port) from January to June 2009.

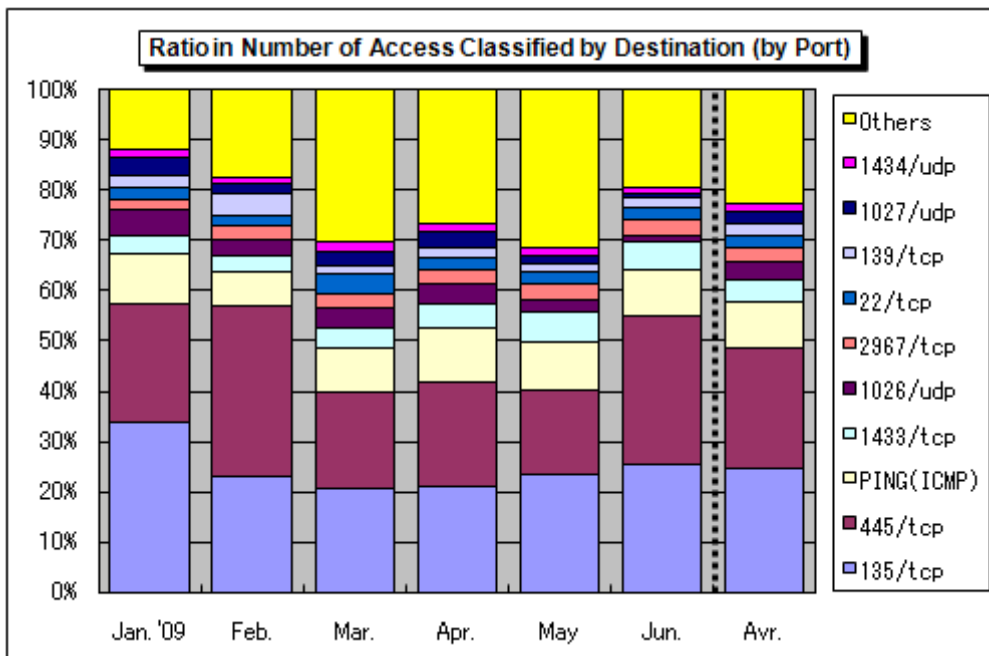


Chart 3-1: Ratio in Number of Access Classified by Destination (by Port) from January to June 2009

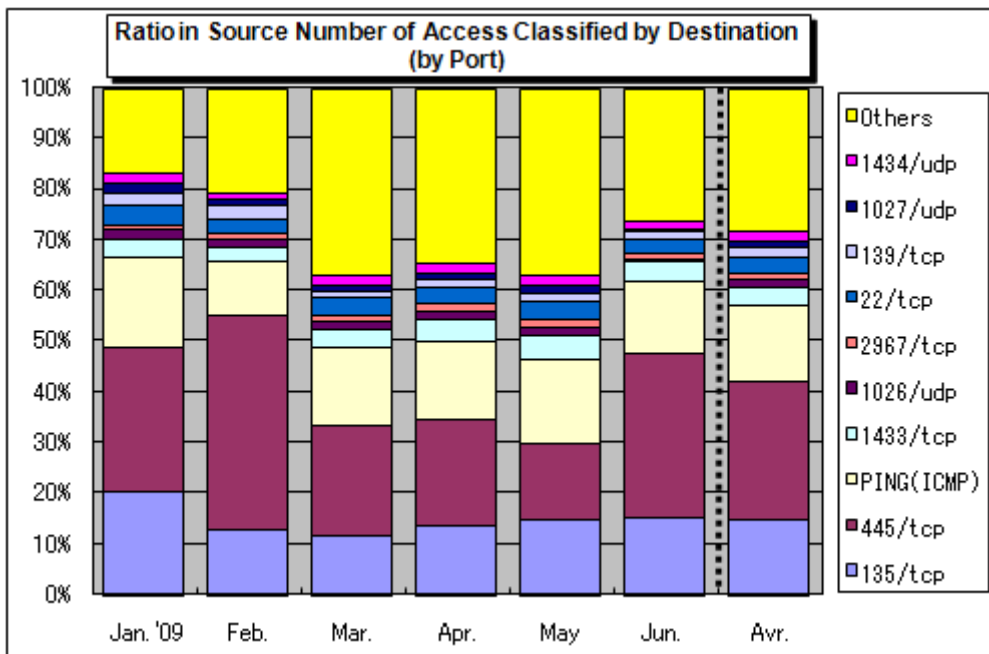


Chart 3-2: Ratio in Source Number of Access Classified by Destination (by Port) from January to June 2009

(2) Ratio Classified by Source Area

The Chart 3-3 shows the ratio in number of access classified by source area and the Chart 3-4 shows the ratio in source number of access classified by source area from January to June 2009.

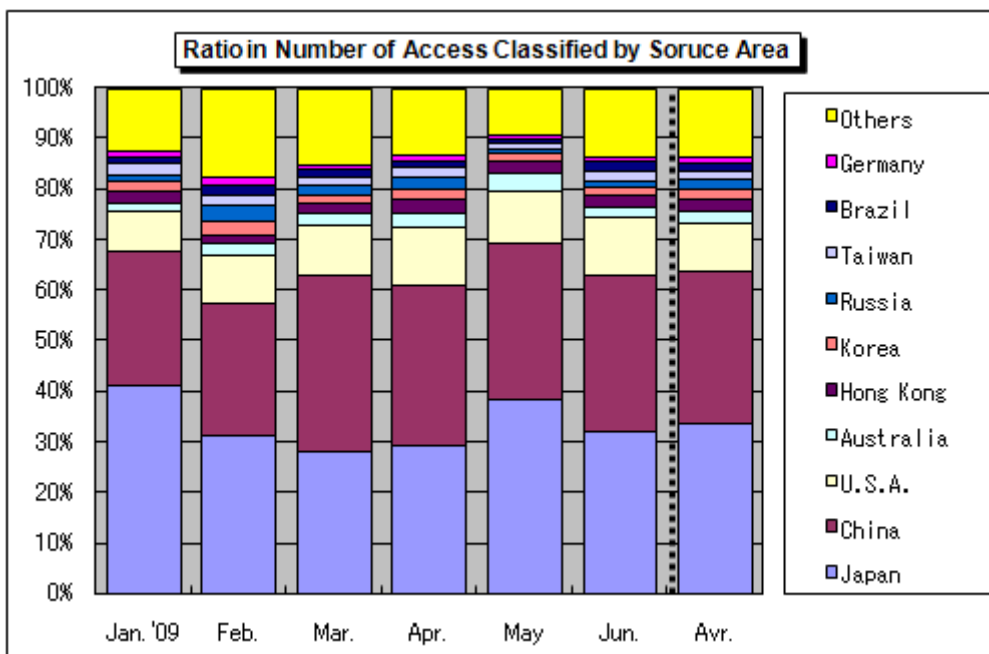


Chart 3-3: Ratio in Number of Access Classified by Source Area from January to June 2009

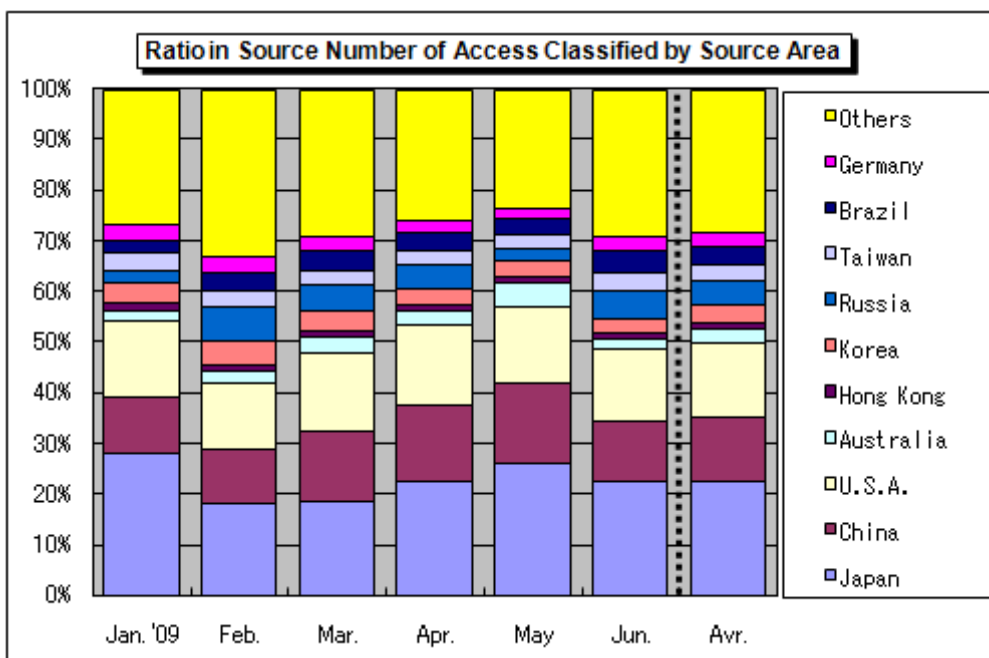


Chart 3-4: Ratio in Source Number of Access Classified by Source Area from January to June 2009

4. Supplementary Descriptions

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in June 2009.

Port Type	Interpretations/Descriptions
Ping (CMP)	This port is originally used to check if the other party or person's computer is in operation and is renowned for being exploited by W32/Welchia, etc. to search to target computers for unauthorized accesses.
22/tcp	The access which targets SSH (Secure Shell: the command execution tool for which security is enough strengthened by encrypting its communication path) to intrude to a system by password cracking attack.
23/tcp	It is probable that this access targets to telnet to intrude to a system by conducting password cracking attack.
135/tcp	This is the default port for the Microsoft Windows Remote Procedure Call (RPC) and is renowned for the unauthorized computer accesses (W32/MSBlaster, etc.) which target vulnerability (MS03-026) relevant to RPC.
139/tcp	Renowned for such unauthorized computer access which targets to a file sharing (i.e., network) for which security is not sufficient: it is probable that this access targets to the vulnerability in Windows.
445/tcp	Renowned for those file sharing (network sharing) that has not been well-protected and unauthorized computer accesses (W32/Sasser, etc.) which targets vulnerabilities specifically in Windows 2000.
1433/tcp	This is the default port for Microsoft SQL Servers which searches those computers for which SQL Server is in operation. The port is also renowned for unauthorized computer access activities which target vulnerabilities in SQL Servers.
1434/udp	Renowned for such unauthorized computer access (W32/SQL Slammer, etc.) which targets the vulnerability in Microsoft SQL Server, etc.
2967/tcp	High potential of access which targets vulnerability in Symantec products such as Symantec Client Security and Symantec AntiVirus, etc.
4899/tcp	Renowned for such unauthorized computer access which targets to the vulnerability in RAdmin for remote operation (RAdmin is the application which enables to remotely operate multiple computers).

Inquiries to:

Information-Technology Promotion Agency, Security Center
 Oura/Hanamura/Kagaya
 Tel.: +81-3-5978-7527
 Fax: +81-3-5978-7518
 E-mail: isec-info@ipa.go.jp