

Report from the Internet Monitoring (TALOT2)

August 2009

1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in June totaled **171,271** cases for the 10 monitoring points and the gross number of the sources* was **65,738**: unwanted (one-sided) access captured at one monitoring point was **552** accesses from **212** sources per day (see the Chart 1-1).

Gross Number of Source (*): Gross number of source refers the total of source number of access summed-up to the respective monitoring points in TALOT2.

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.

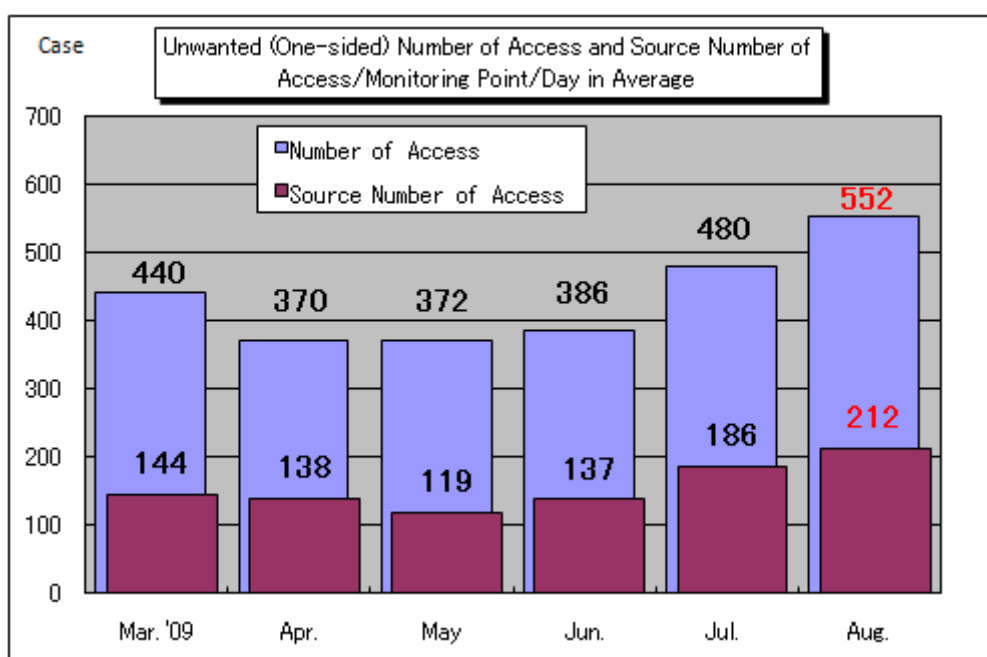


Chart 1-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day

The Chart 1-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day in average from March to August 2009. Both the number of access and the source number of access were increased compared with those in July.

The Chart 1-2 shows the comparison in number of access classified by destination (by port) in July and August. The number of access significantly increased in August was the access to the port 445/tcp. Though the number of access from specific source was not increased, the entire number of access was increased by the number of access to the port 445/tcp. In August, the number of access to the port 39023/tcp which had never been monitored in July could be observed frequently. We cannot identify what did this access purpose for: this access was only monitored at single monitoring point.

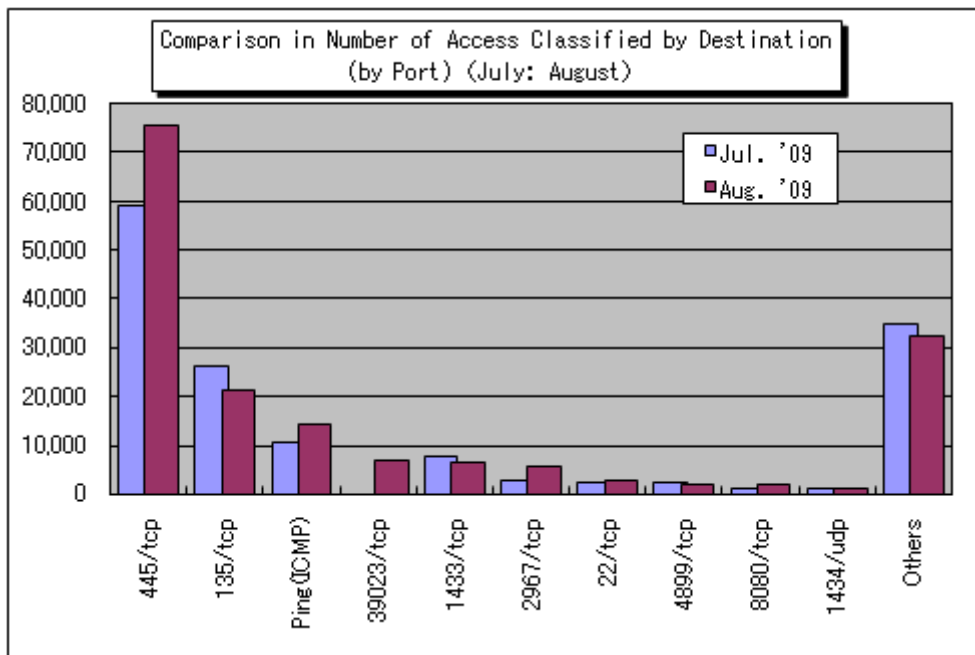


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (July: August)

As you can see the Chart 5-1, the number of access/monitoring point/day in average tended to gradually increase over the past 4 months. The Chart 5-3 shows the shift in number of access to the top 10 ports (i.e., the worst 10 ports) frequently accessed over the past 4 months.

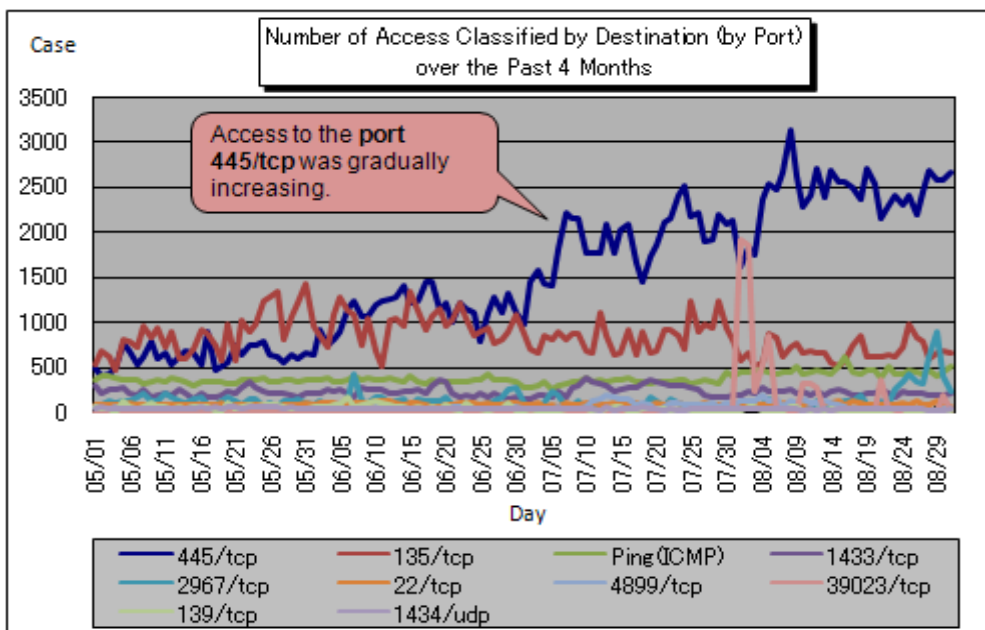


Chart 1-3: Number of Access to the Port 445/tcp Classified by Destination (by Port) over the Past 4 Months

According to this chart, while the number of access to the most of all ports was shifted by maintaining certain level, yet the number of access to the port 445/tcp was gradually increasing: it can be seen that the access to this port made to increase the entire number of access in average significantly.

Since the port 445/tcp was renowned as the port to be exploited when conducting attacks targeting vulnerability in Windows; however, the cause why it has been increasing and been monitored by the TALOT2 for such a long period has not yet been identified.

2. Unwanted (One-sided) Number of Access in August 2009

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

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

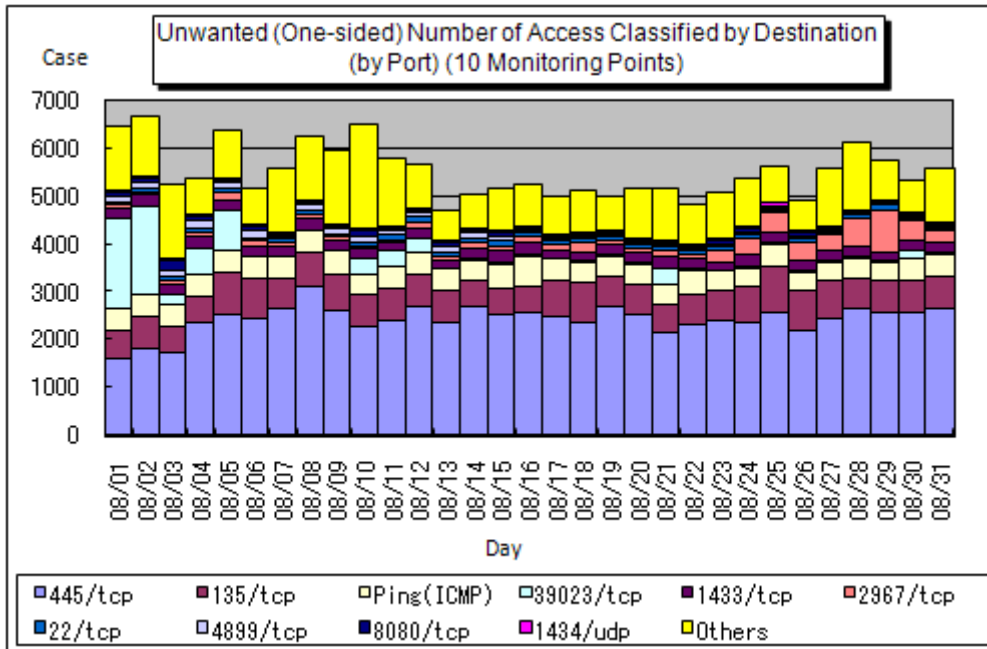


Chart 2-1: Number of Access Classified by Destination (by Port)/Day in August 2009

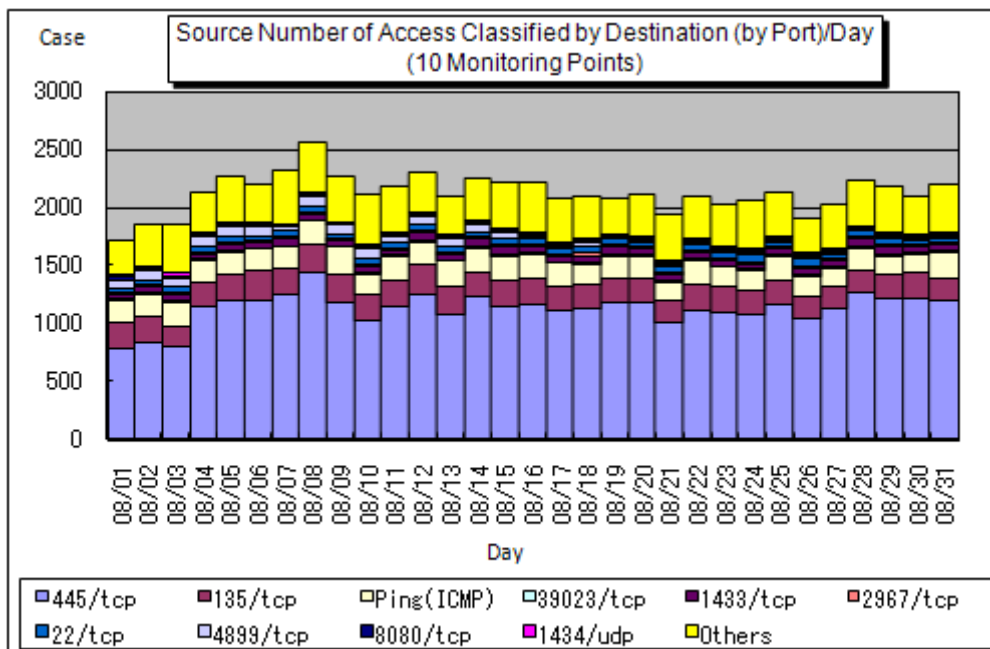


Chart 2-2: Source Number of Access Classified by Destination (by Port)/Day in August 2009

(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 August 2009. In addition, numbers in ratio are rounded at the 1st arithmetic point so that they may not make 100% sharp, accordingly.

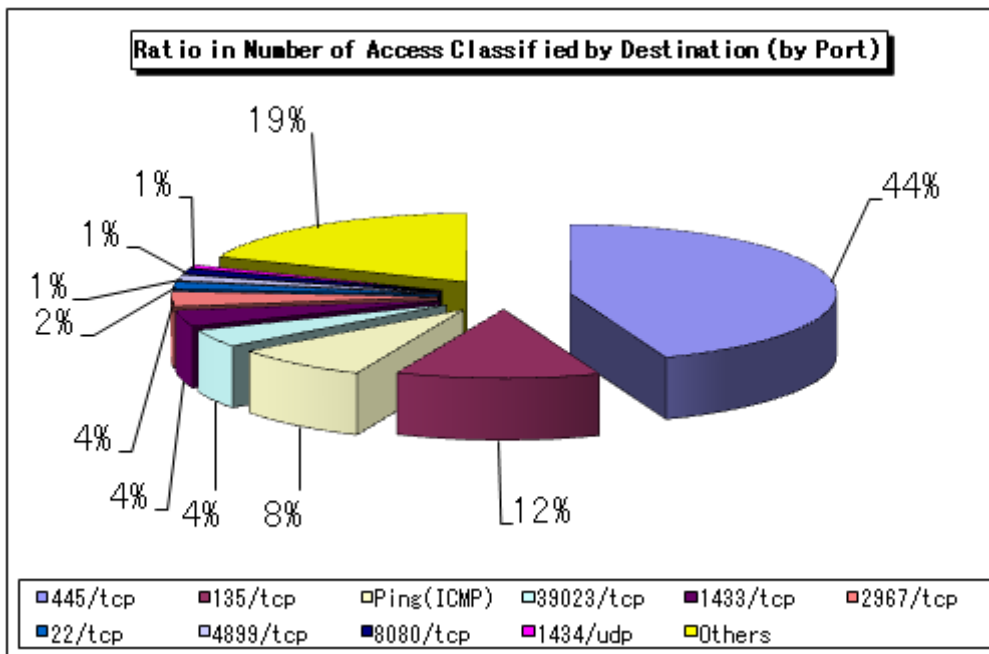


Chart 2-3: Ratio in Number of Access Classified by Destination (by Port) in August 2009

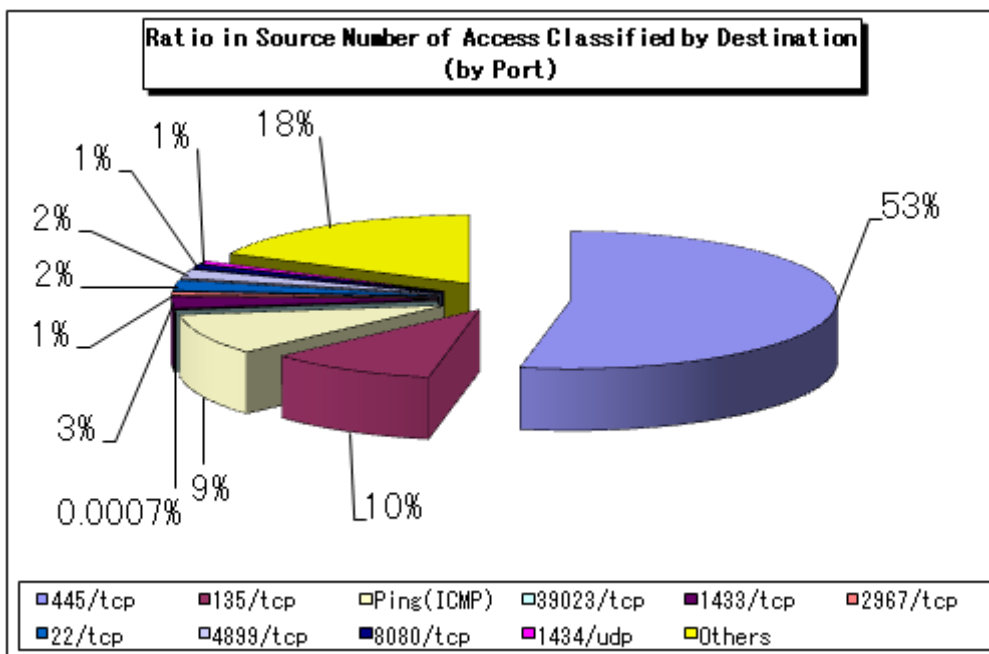


Chart 2-4: Ratio in Source Number of Access Classified by Destination (by Port) in August 2009

(3) Accessing Status Classified by Source Area

The Chart 2-5 shows the shift in number of access classified by source area and the Chart 2-6 shows the ratio in number of access classified by source area in August 2009. In addition, numbers in ratio are rounded at the 1st arithmetic point so that they may not make 100% sharp, accordingly.

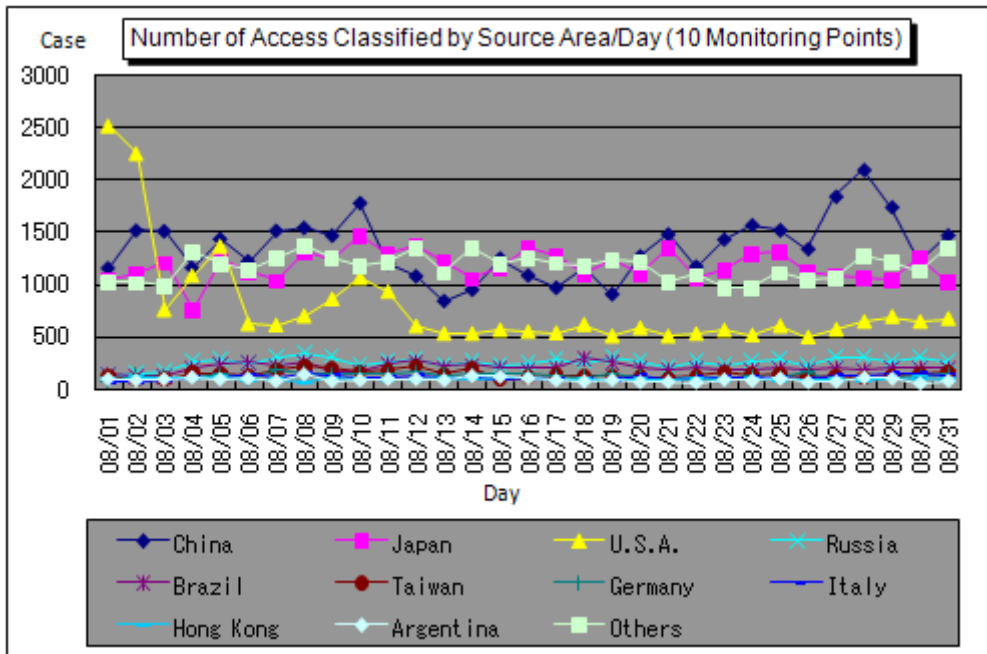


Chart 2-5: Number of Access Classified by Source Area/Day in August 2009

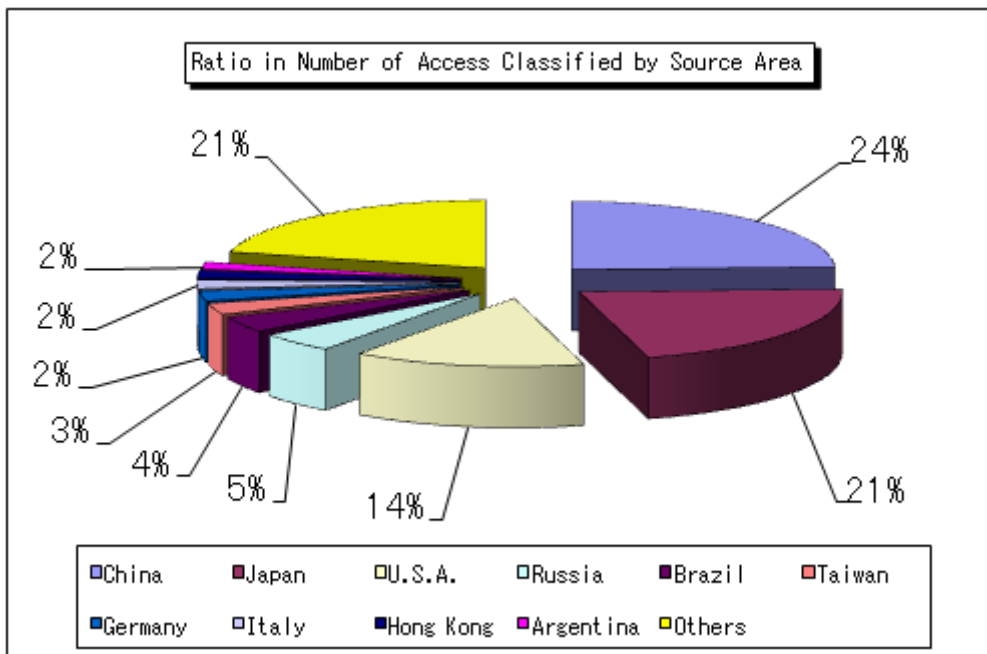


Chart 2-6: Ratio in Number of Access Classified by Source Area in August 2009

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 August 2009. In addition, numbers in ratio are rounded at the 1st arithmetic point so that they may not make 100% sharp, accordingly.

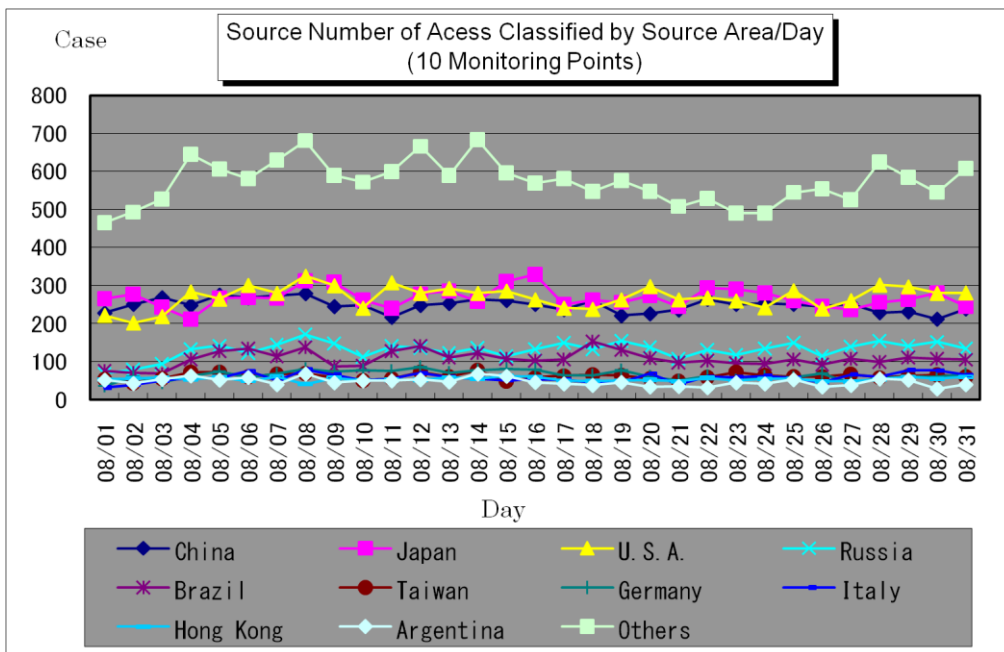


Chart 2-7: Source Number of Access Classified by Source Area/Day in August 2009

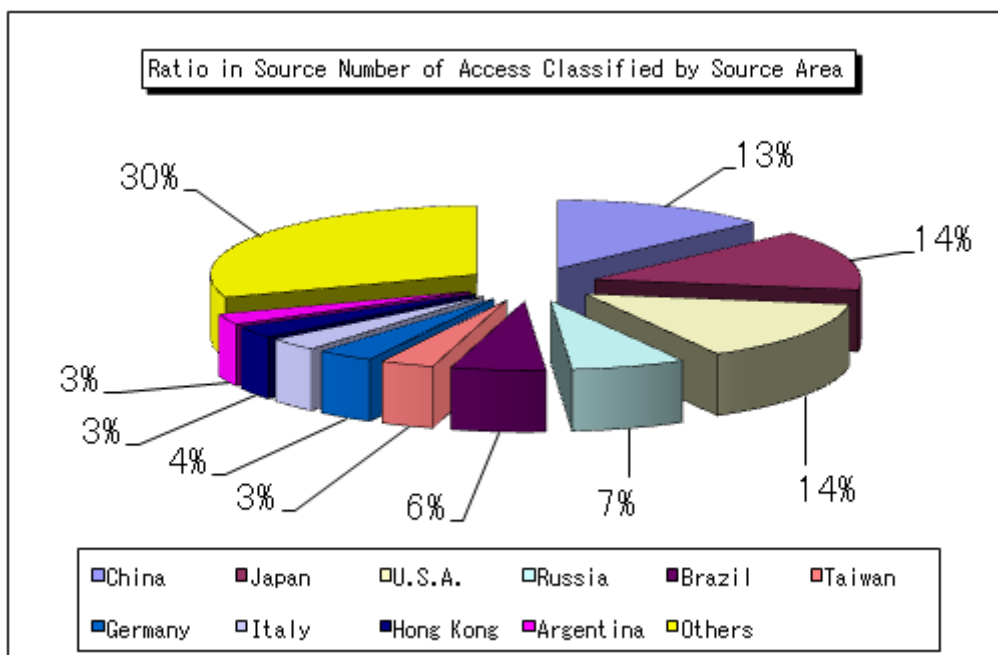


Chart 2-8: Ratio in Source Number of Access Classified by Source Area in August 2009

3. Statistical Information

(1) Ratio Classified by Destination (by Port)

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 March to August 2009.

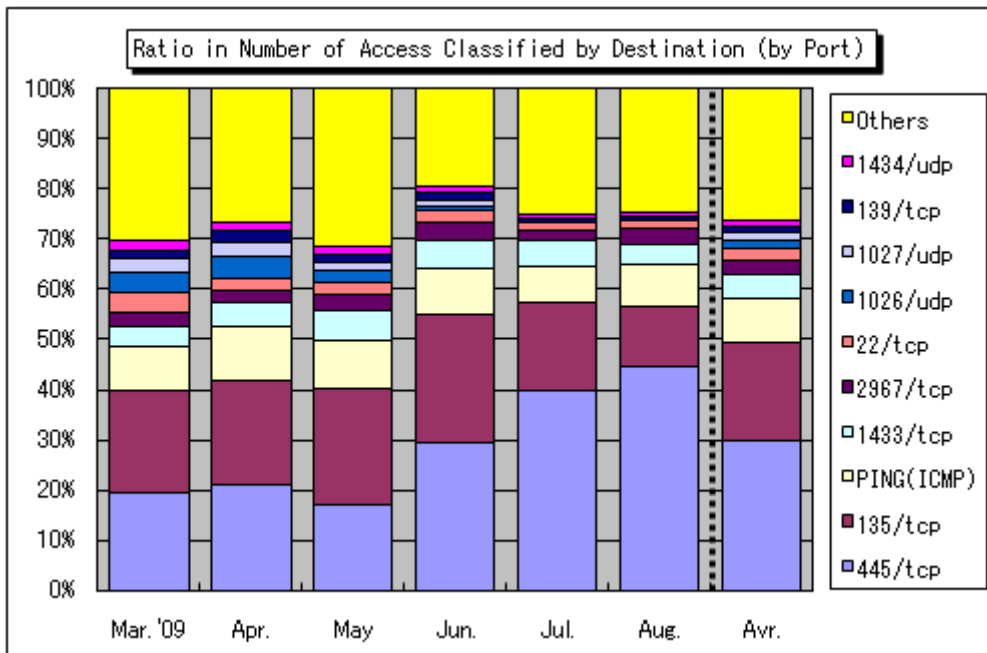


Chart 3-1: Ratio in Number of Access Classified by Destination (by Port) from March to August 2009

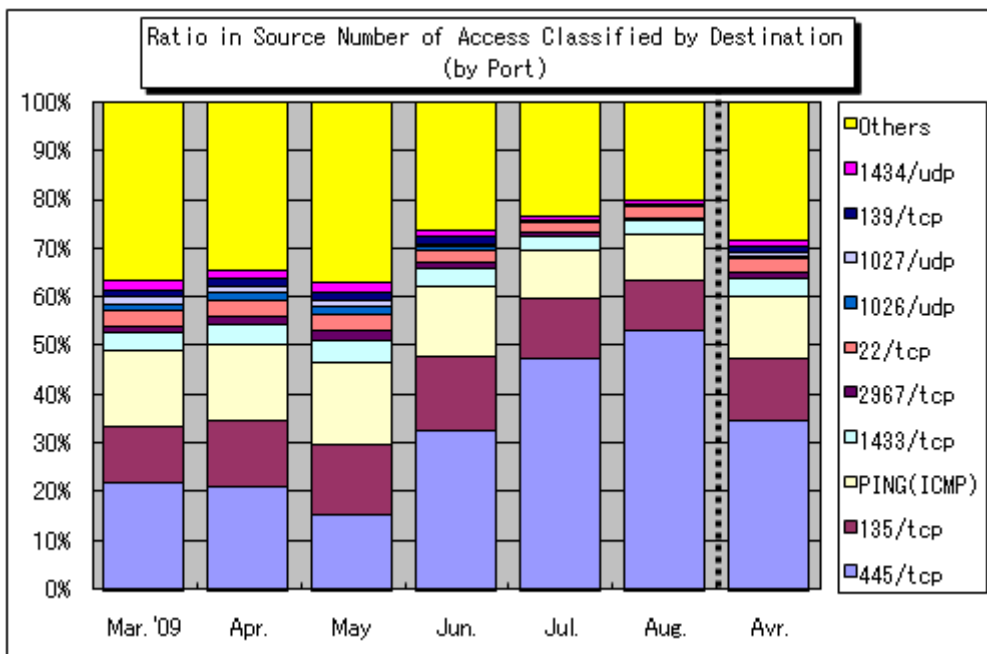


Chart 3-2: Ratio in Source Number of Access Classified by Destination (by Port) from March to August 2009

(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 March to August 2009.

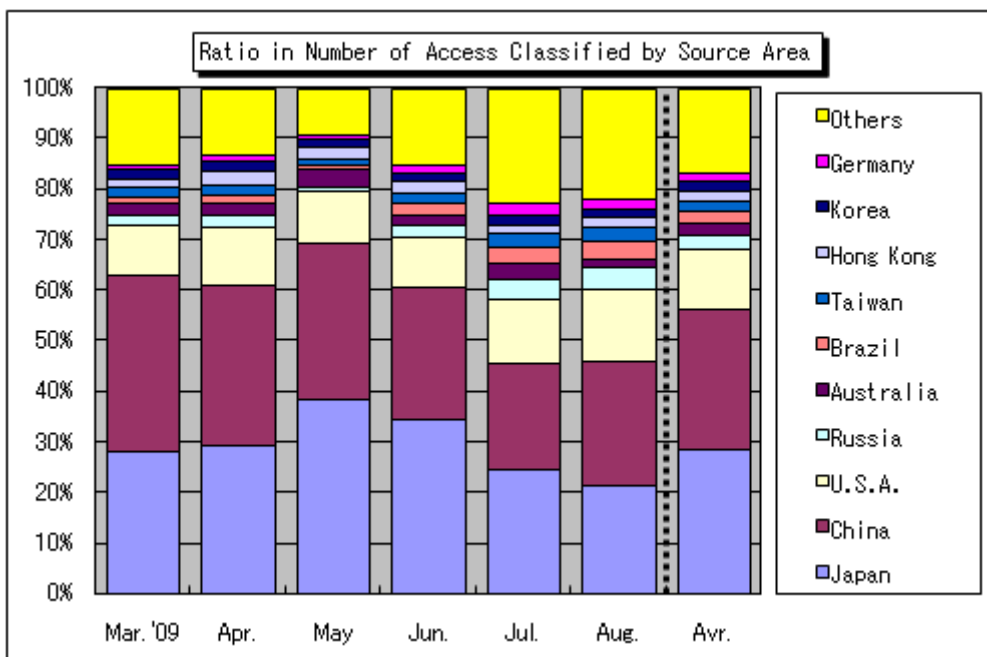


Chart 3-3: Ratio in Number of Access Classified by Source Area from March to August 2009

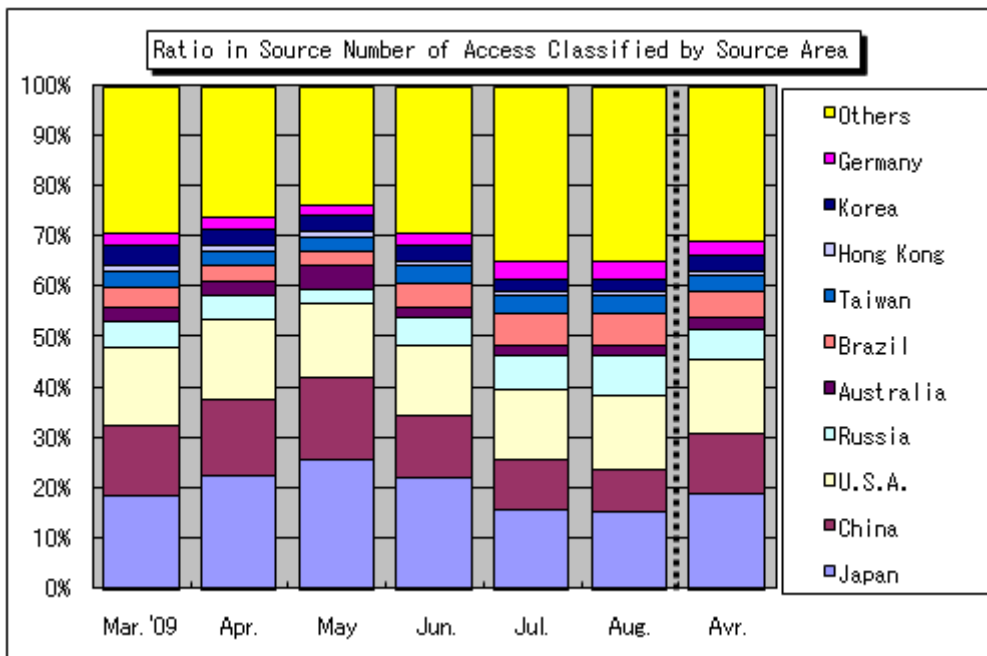


Chart 3-4: Ratio in Source Number of Access Classified by Source Area from March to August 2009

4. Supplementary Explanations

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in August 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.
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.
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/tcp	Renowned by unauthorized computer access targeting the vulnerability (by W32/SQL Slammer) 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).
8080/tcp	This is the frequently accessed port to connect to HTTP Proxy: it is probable that the port is exploited by malicious intent when he/she explores such proxy server (s) which is available to use the steppingstone to access fraudulently.
39023/tcp	Unknown access: this was monitored only at specific and single monitoring point.

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