

Report from the Internet Monitoring (TALOT2)

November 2009

1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in November totaled **172,802** cases for the 10 monitoring points and the gross number of the sources* was **71,136**: unwanted (one-sided) access captured at one monitoring point was **576** accesses from **237** 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.

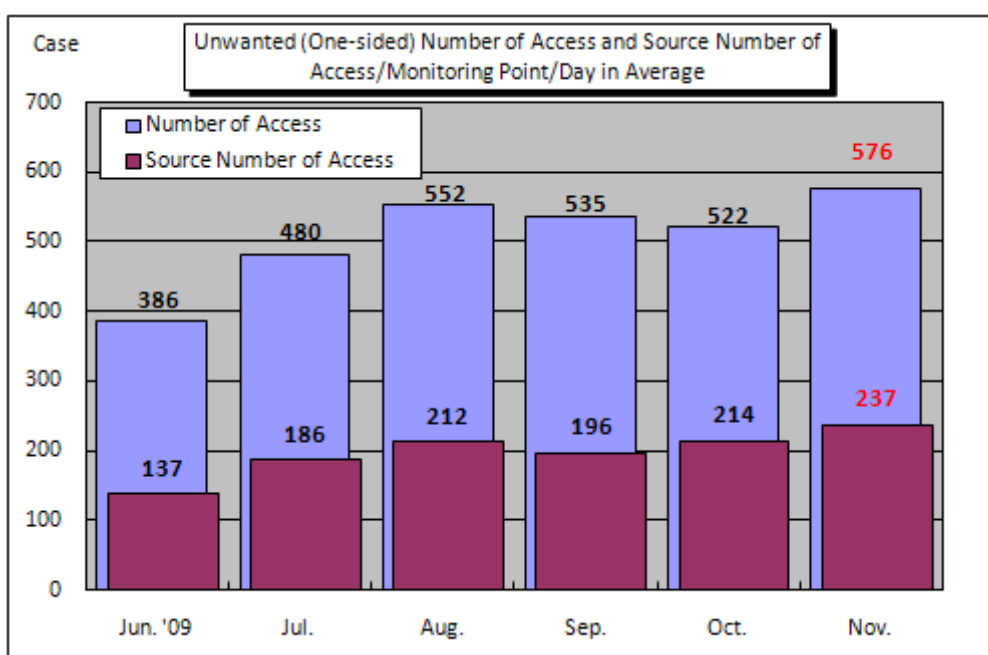


Chart1-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day/in Average

The Chart 1-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day in average from June to November 2009. Both the unwanted (one-sided) number of accesses were increased from the ones marked in October.

The Chart 1-2 shows the comparison in number of access by destination (by port) in October and November. In November, the number of access was entirely increased with several reasons: The one was the number of access to the port 60304/udp was frequently monitored (in October none of such access was monitored). The other one was the number of access to the several ports such as 2967/tcp, 139/tcp, 1521/tcp, etc. were increased.

The access to the port 60304/udp was monitored only in couple of days in the last part of November and the source was only from Australia. We cannot identify their purpose (s) of access. In addition, the number of access to the port 1521/tcp had proportionally increased the most compared with the one in October. The port 1521/tcp is the default port used by Oracle database. In TALOT2, the access increase to this port having been monitored on and around the first part of July in 2009 and the number of access was subtly increased from the last part of October as well (See the Chart 1-3). This can be monitored in several organizations who also conduct the Internet monitoring activities. We identified the site in China which

distribute such tool that can scan the port 1521/tcp in the first part of July: since the access increase to this port was initially monitored on and around the first part of July; we parsed that there may have been continually accessed to the port to probe vulnerable Oracle database by using this tool.

To prevent from such access increase, following countermeasures will be of help.

- Restricting access from outside/restricting connectable IP address by firewall
- The default port number assigned for Oracle database changes to different port number
- Reconfigure the user's password for the Oracle database to the one hardly assumable
- Resolve vulnerabilities in OSs and the other application software

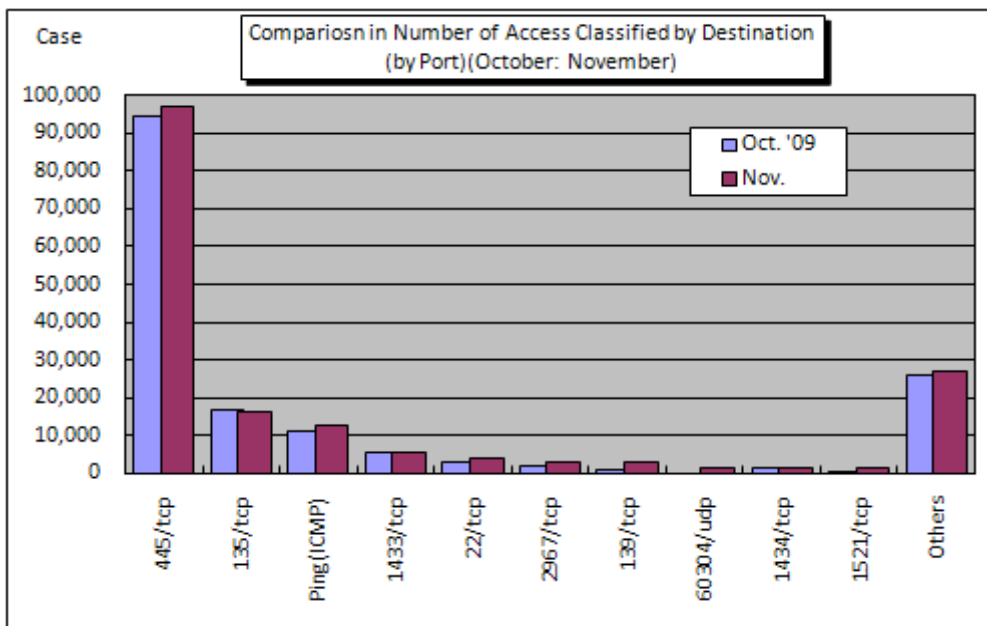


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (October: November)

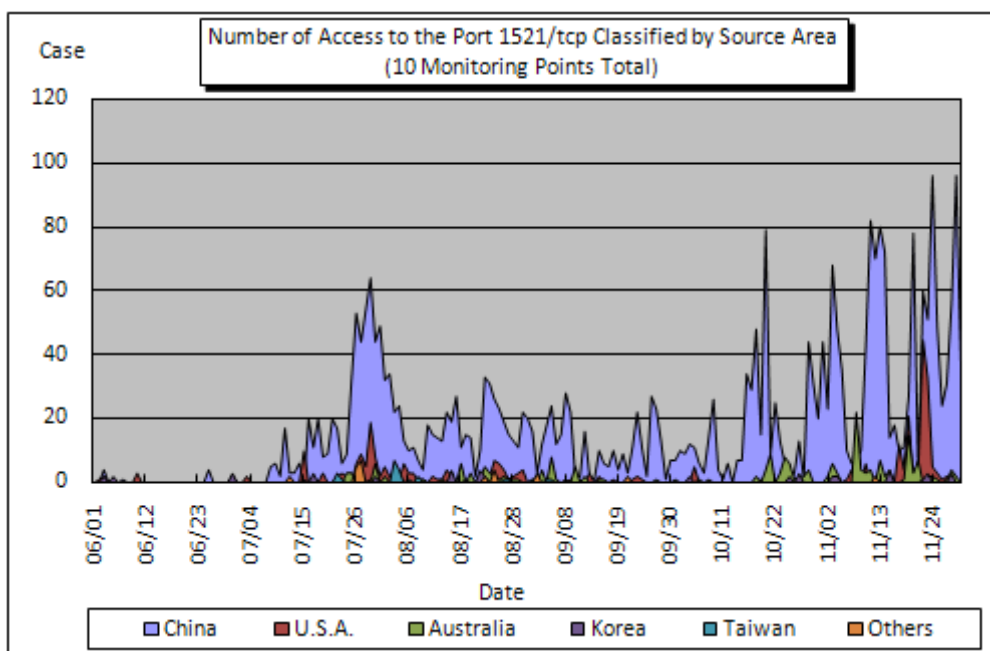


Chart 1-3: Number of Access Classified by Source Area (10 Monitoring Points Total)

2. Status for Unwanted (One-sided) Number of Access in November 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 November 2009.

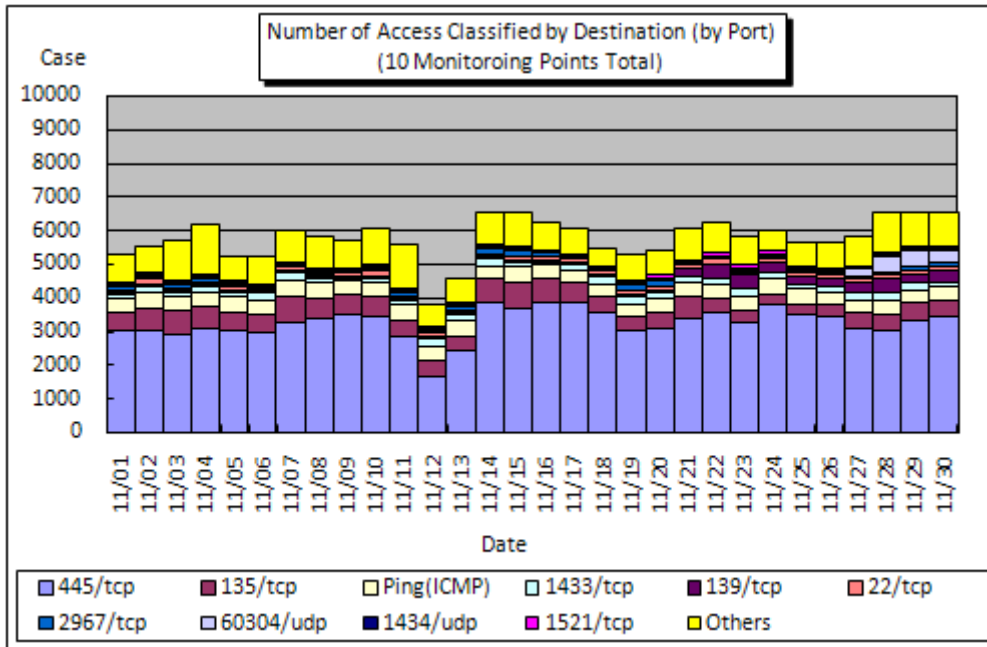


Chart 2-1: Number of Access Classified by Destination (by Port)/Day in November 2009

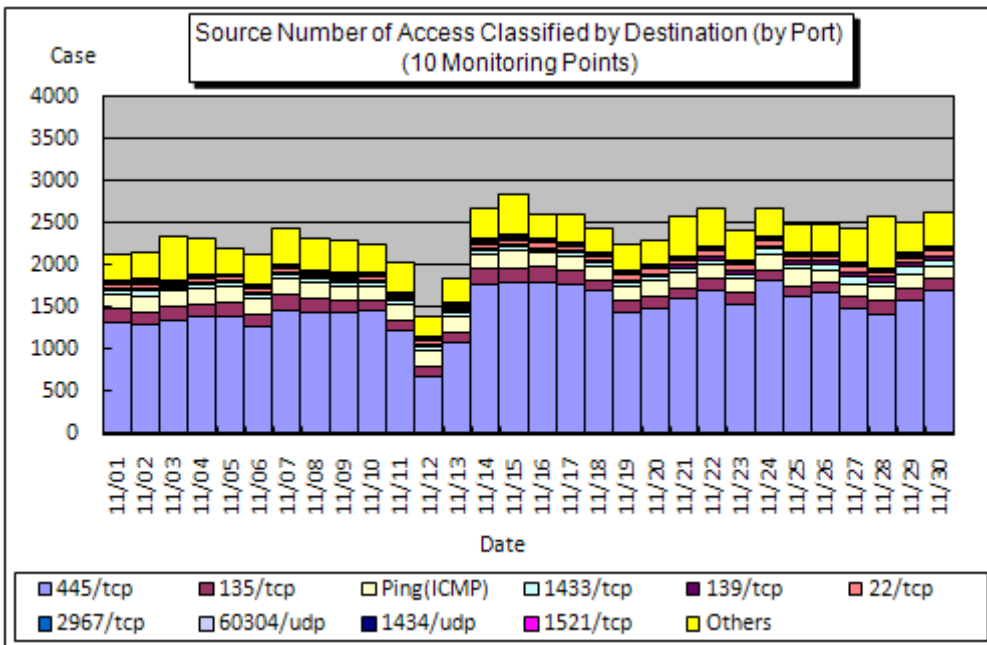


Chart 2-2: Source Number of Access Classified by Destination (by Port)/Day in November 2009

(2) Ratio in 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 November 2009. For your further information, numbers in ratio were rounded at the 1st arithmetic point so that their total may not make 100% sharp, accordingly.

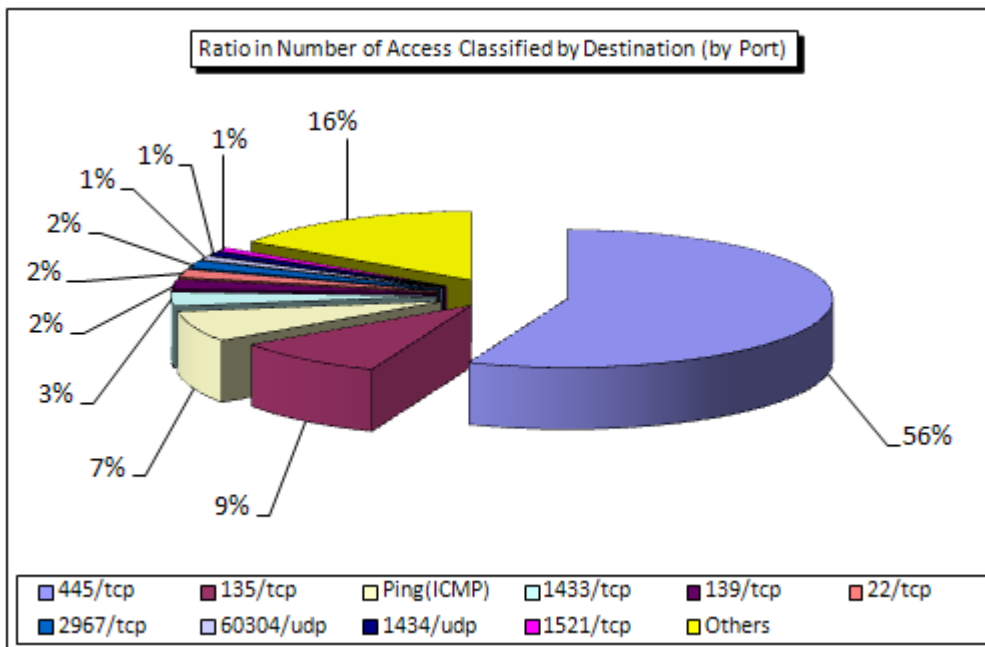


Chart 2-3: Ratio in Number of Access Classified by Destination (by Port) in November 2009

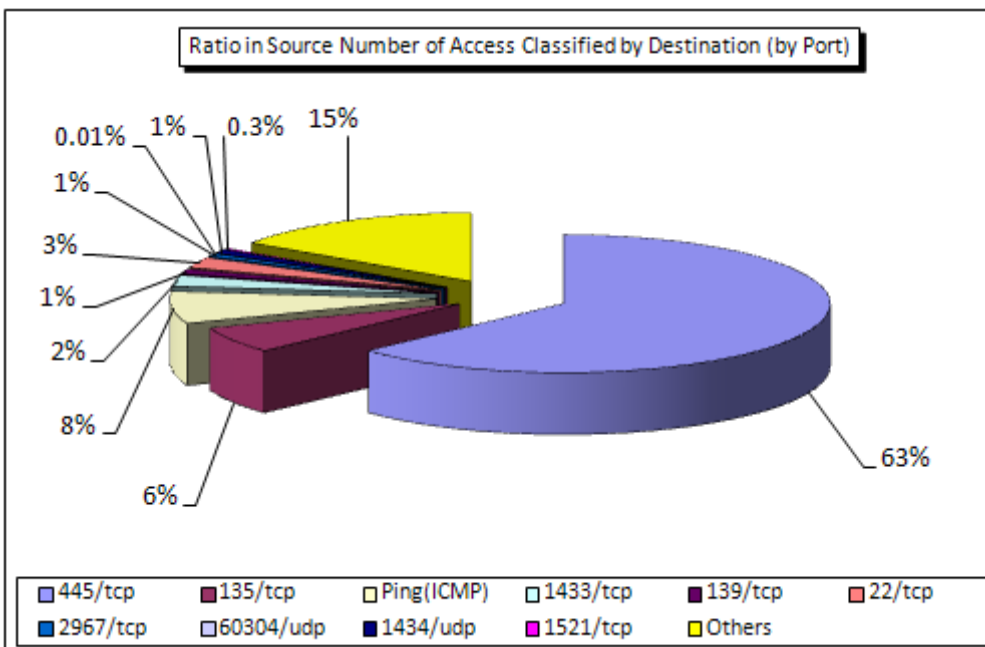


Chart 2-4: Ratio in Source Number of Access Classified by Destination (by Port) in November 2009

(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 November 2009. For your further information, numbers in ratio were rounded at the 1st arithmetic point so that their total may not make 100% sharp, accordingly.

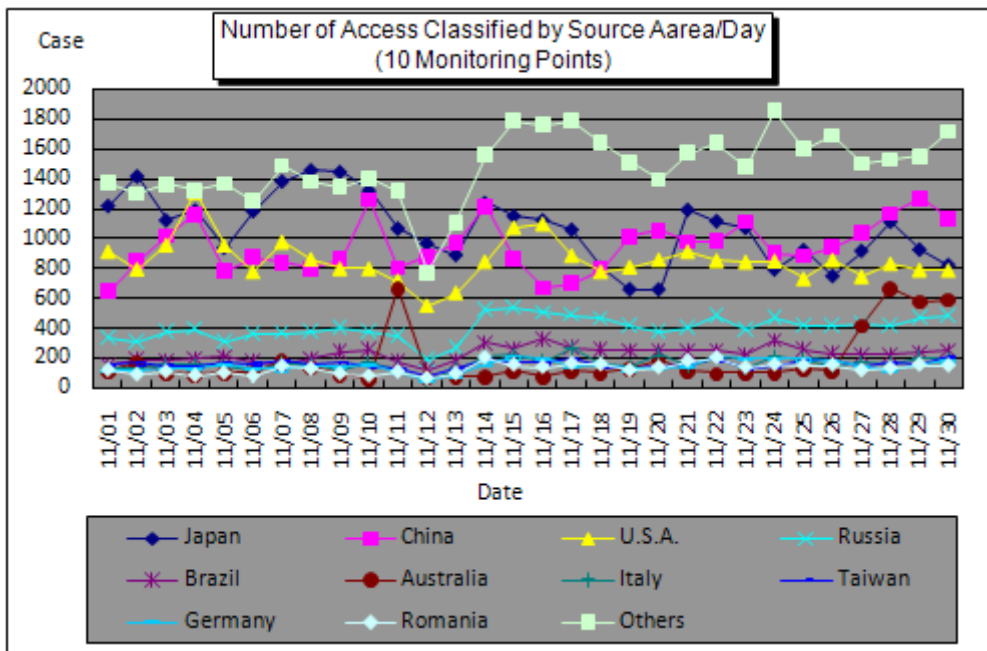


Chart 2-5: Number of Access Classified by Source Area/Day in November 2009

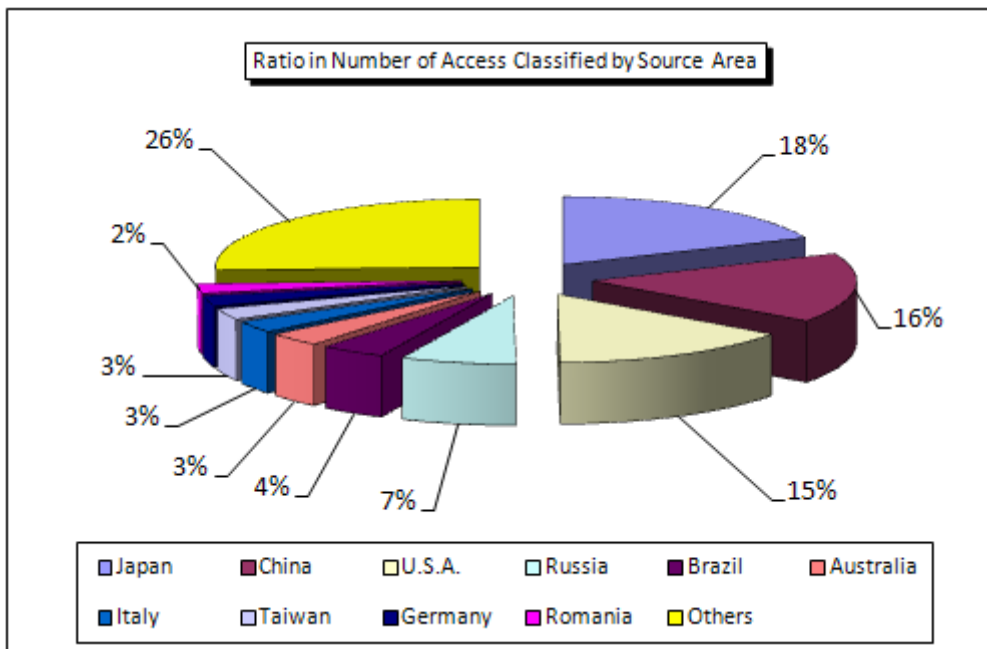


Chart 2-6: Ratio in Number of Access Classified by Source Area in November 2009

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 November 2009. For your further information, the numbers in ratio were rounded at the 1st arithmetic point so that their total may not make 100% sharp, accordingly.

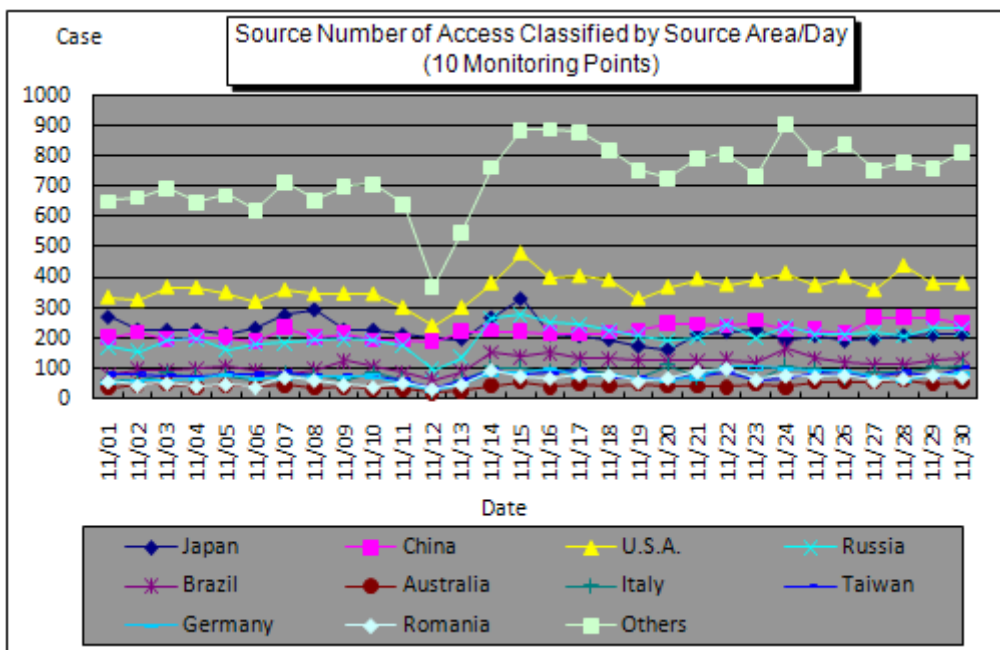


Chart 2-7: Source Number of Access Classified by Source Area/Day in November 2009

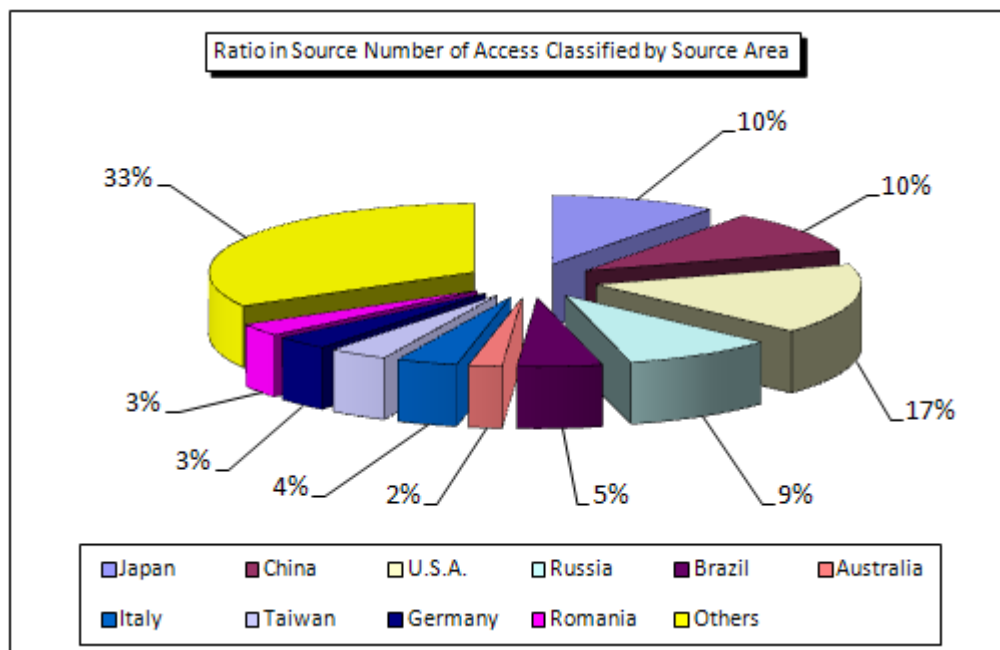


Chart 2-8: Ratio in Source Number of Access Classified by Source Area in November 2009

3. Statistical Information

(1) Ratio in 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 June to November 2009.

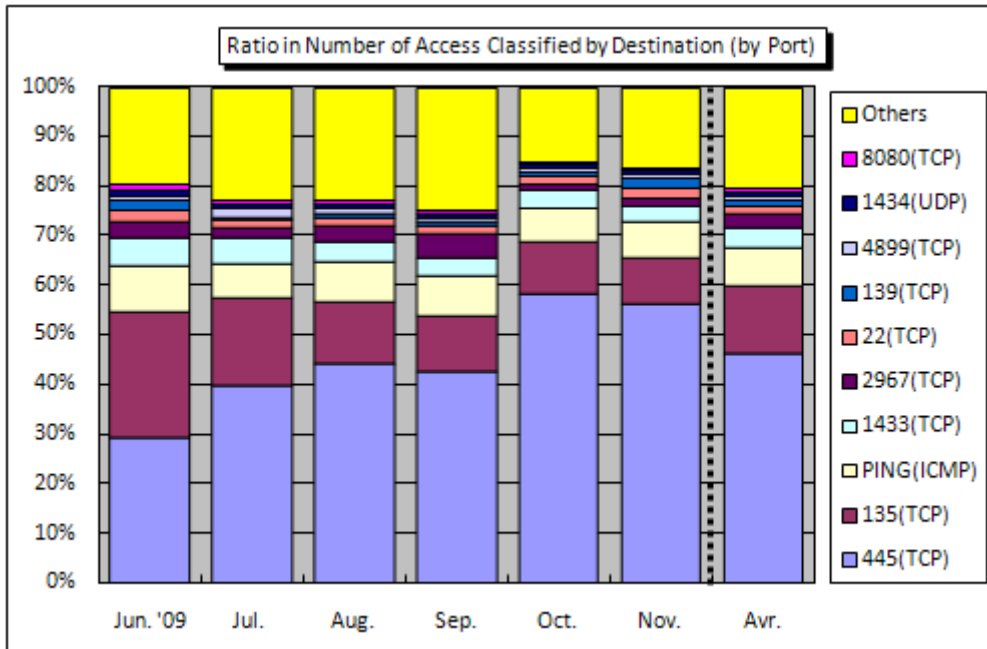


Chart 3-1: Ratio in Number of Access Classified by Destination (by Port) from Jun. to Nov. 2009

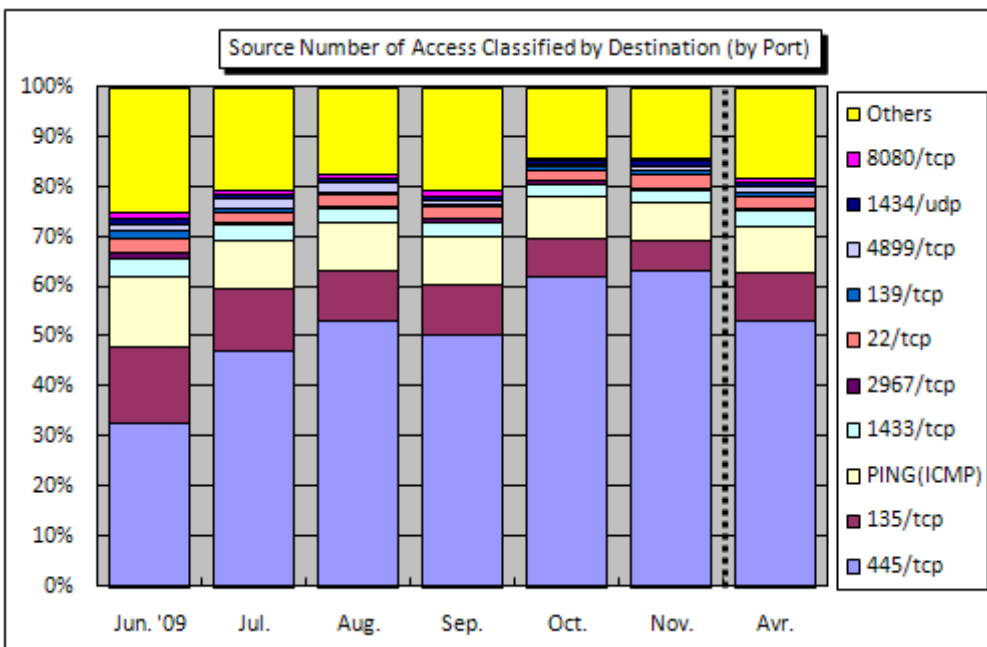


Chart 3-2: Ratio in Source Number of Access Classified by Destination (by Port) from Jun. to Nov. 2009

(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 June to November 2009.

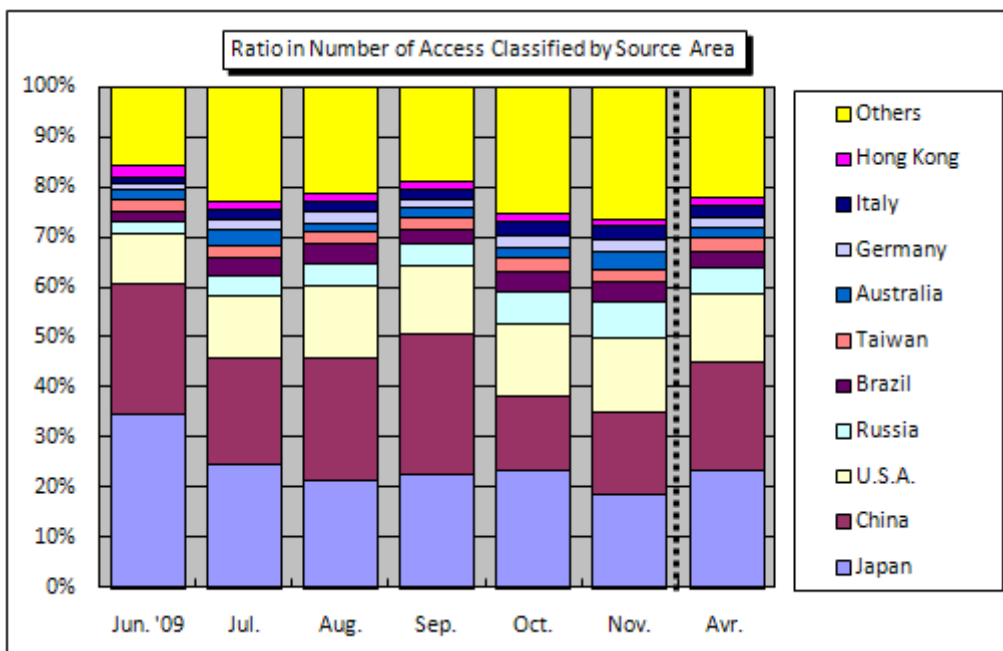


Chart 3-3: Ratio in Number of Access Classified by Source Area from Jun. to Nov. 2009

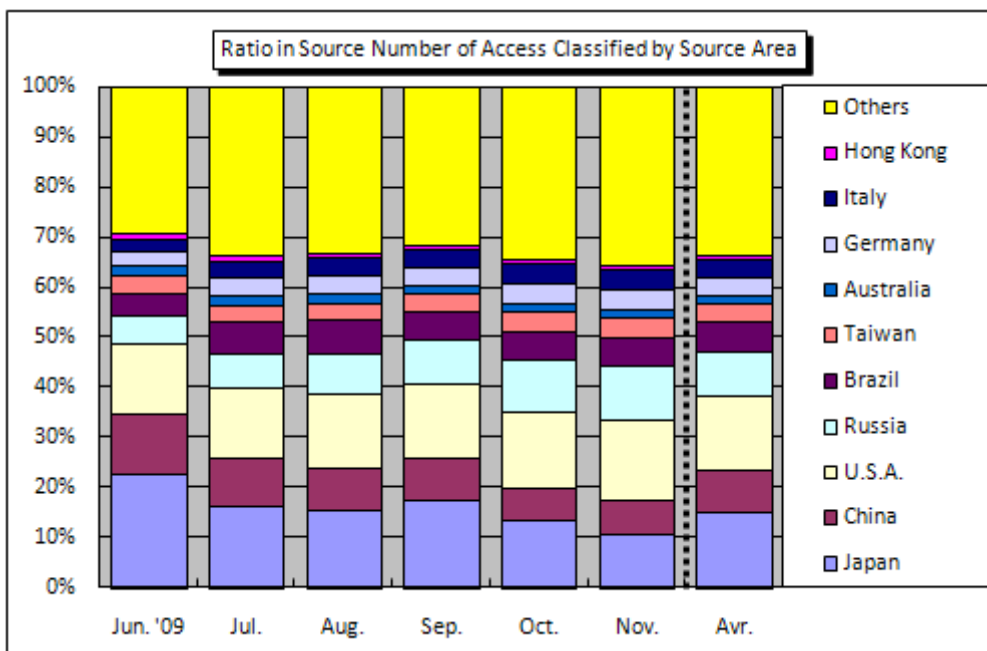


Chart 3-4: Ratio in Source Number of Access Classified by Source Area from Jun. to Nov. 2009

4. Supplementary Explanations

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

Port Type	Interpretations/Descriptions
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.
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.
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.
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.
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.
2967/tcp	High potential of access which targets vulnerability in Symantec products such as Symantec Client Security and Symantec AntiVirus, etc.
139/tcp	Renowned by unauthorized computer access targeting the file (network) sharing for which security is insufficient; this port is frequently targeted by those accesses which target vulnerability in Windows.
60304/tcp	The access from a certain source only monitored by single monitoring point: the cause is not unknown.
1434/tcp	Renowned by unauthorized computer access targeting the vulnerability (by W32/SQL Slammer) in Microsoft SQL Server, etc.
1521/tcp	This is the default port used by Oracle database. This access was highly probable to probe to vulnerable Oracle database using specific tool (s).

Inquiries to:

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