

Report from the Internet Monitoring (TALOT2)

January 2010

1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in January totaled **185,488** cases for the 10 monitoring points and the gross number of the sources* was **78,209**: unwanted (one-sided) access captured at one monitoring point was **598** accesses from **252** 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.

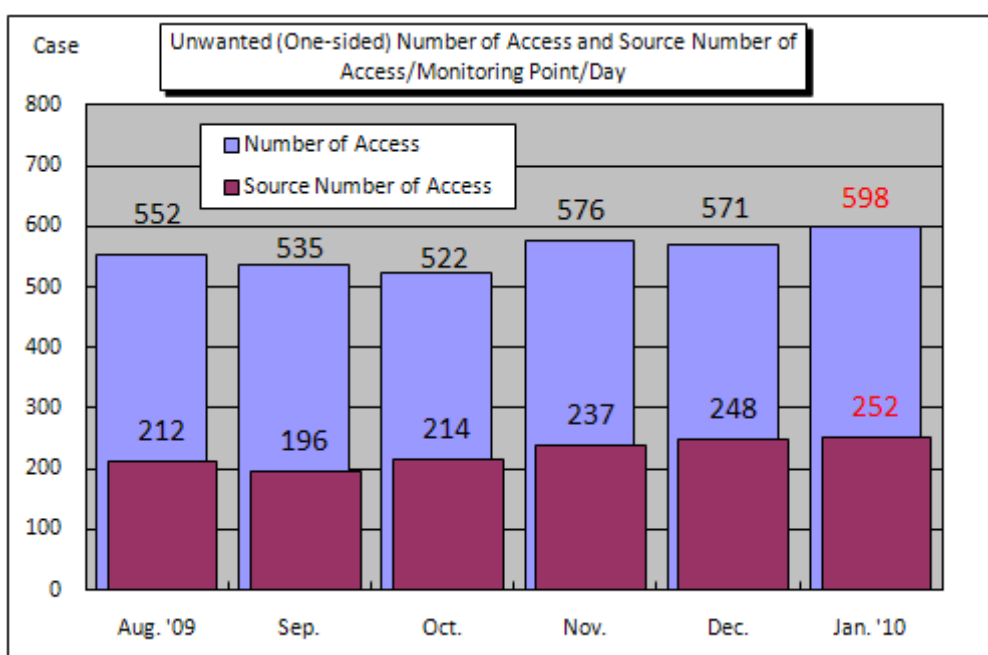


Chart 1-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 1-1 shows the unwanted (one-sided) number of access and source number of access/monitoring point/day in average from August 2009 to January 2010. Both unwanted (one-sided) number of access and source number of access were increased from December 2009.

The Chart 1-2 shows the comparison of number of access classified by destination (by port) for December 2009 and January 2010. According to this chart, accesses to the port 445/tcp was increased, but the accesses to the other ports were shifted with the same level from December 2009.

In the TALOT2 monitoring environment, accesses to the port 445/tcp are remarkably many than the other ports; it is necessary to watch over as this port is still easily targeted by malicious intents.

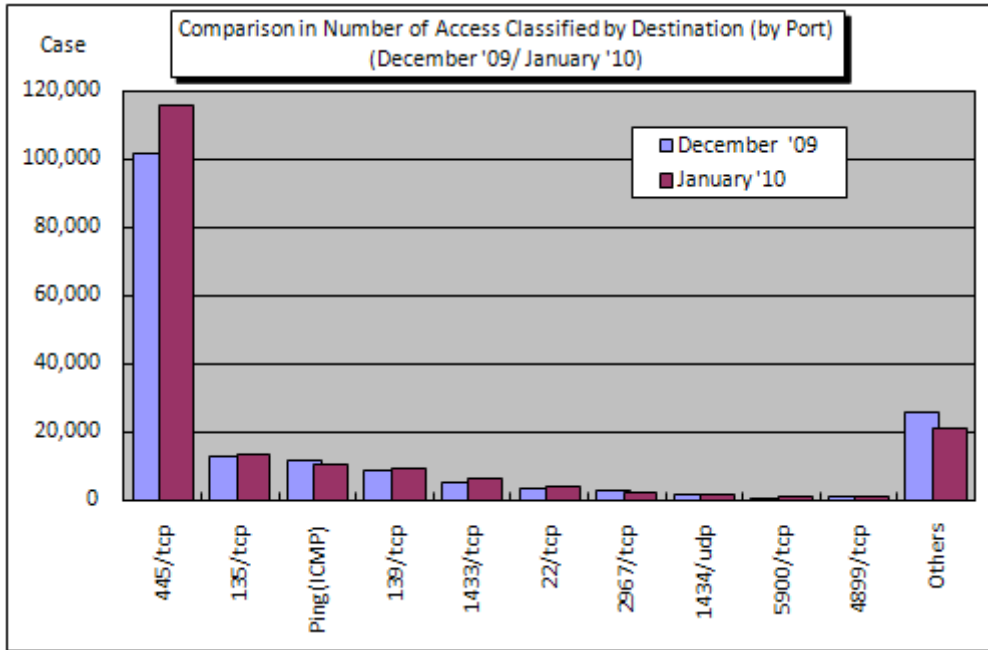


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (December '09/January '10)

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

(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 January 2010.

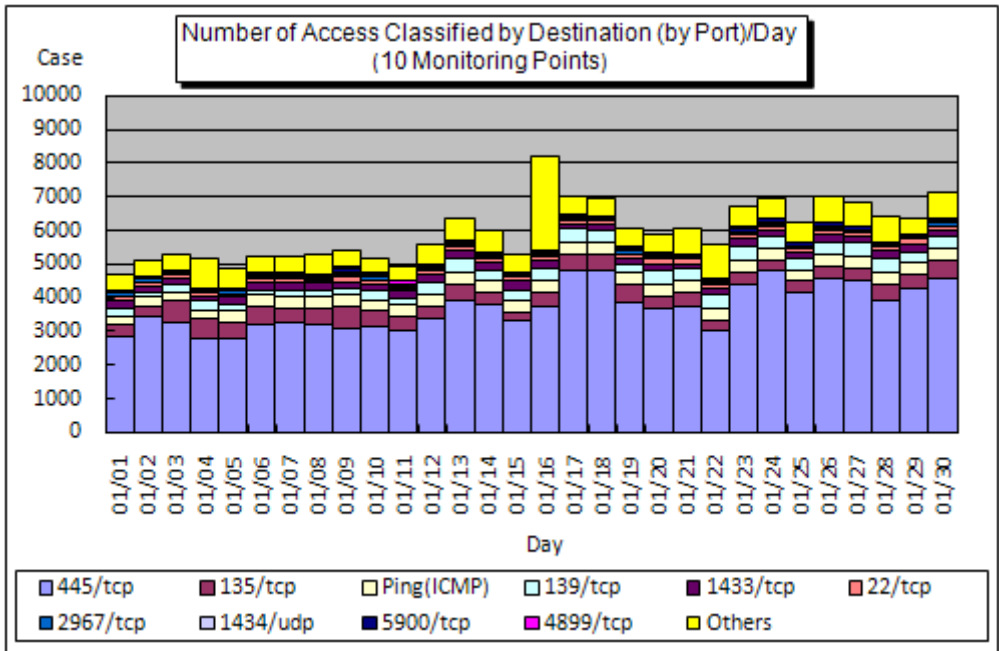


Chart 2-1: Number of Access Classified by Destination (by Port)/Day in January 2010

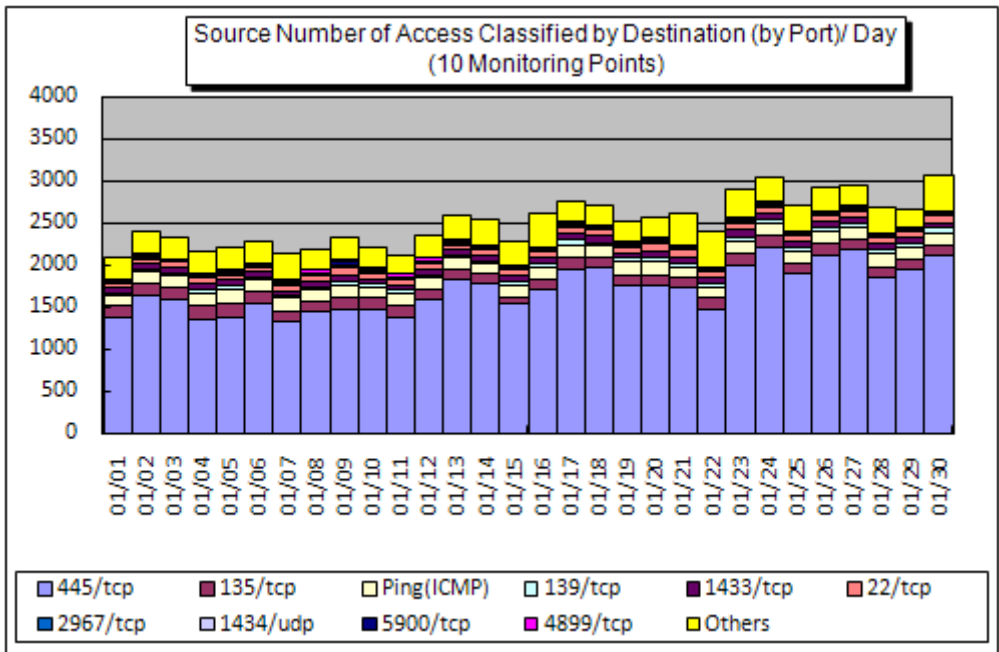


Chart 2-2: Source Number of Access Classified by Destination (by Port)/Day in January 2010

(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 January 2010. For your further information, numbers in ratio were rounded at the 1st arithmetic point so that their total may not make 100% sharp, accordingly.

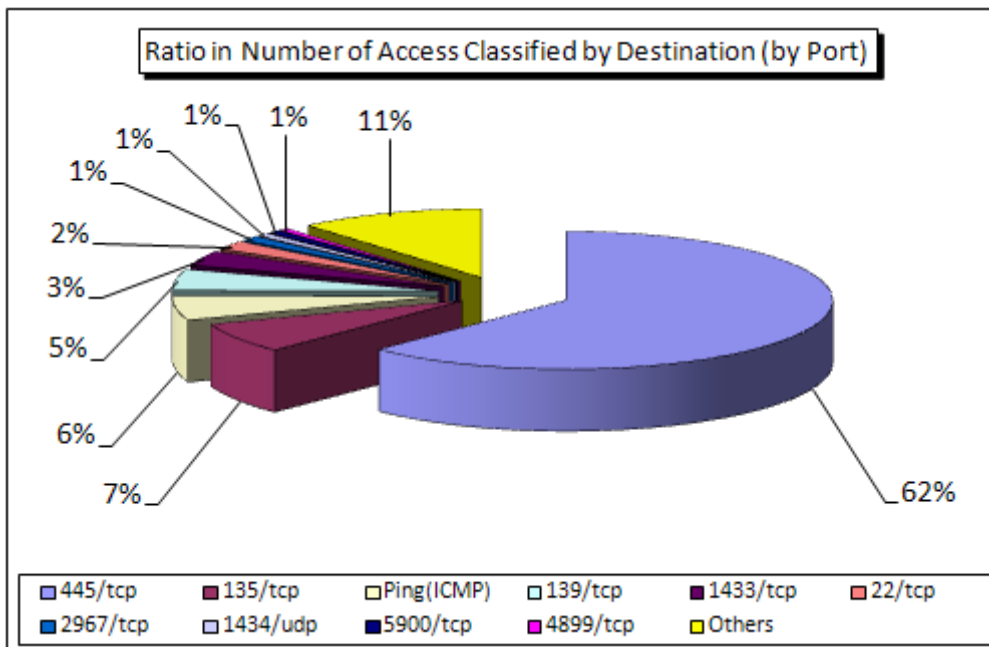


Chart 2-3: Ratio in Number of Access Classified by Destination (by Port) in January 2010

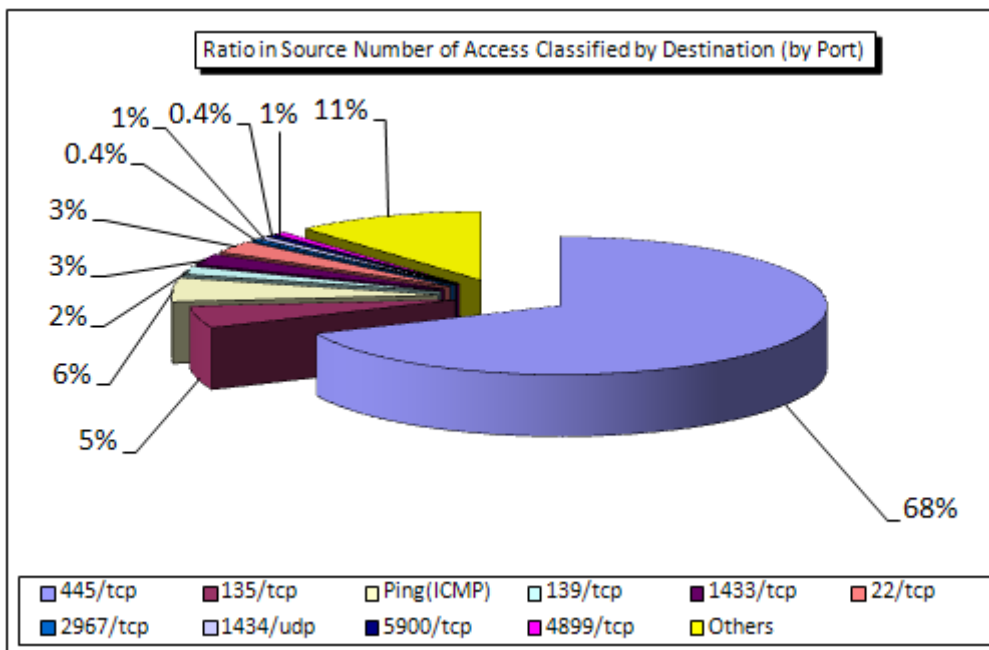


Chart 2-4: Source Number of Access Classified by Destination (by Port) in January 2010

(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 January 2010. For your further information, numbers in ratio were rounded at the 1st arithmetic point so that their total may not make 100% sharp, accordingly.

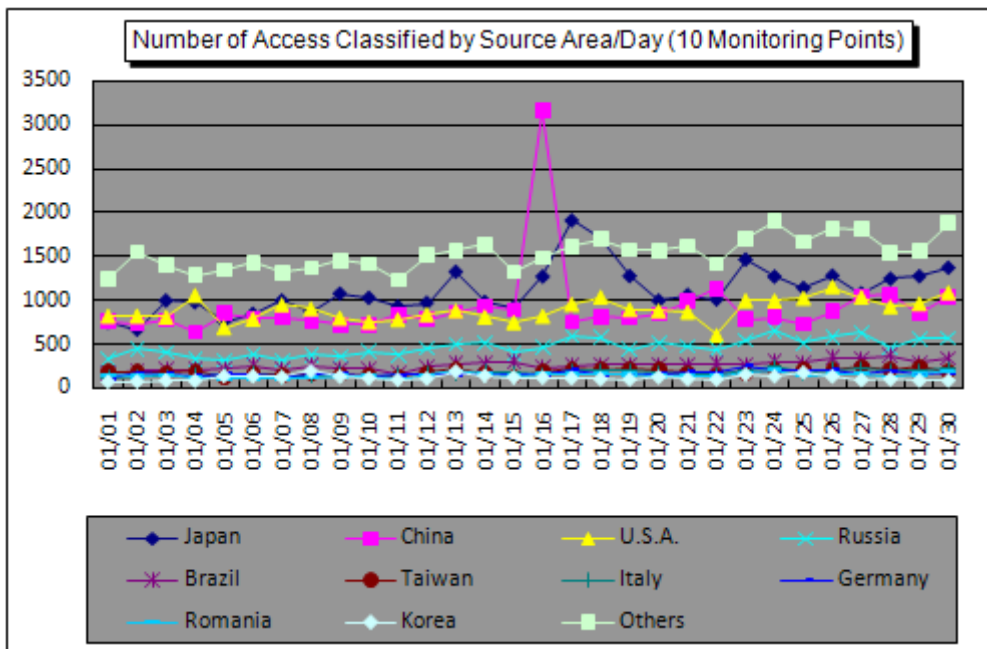


Chart 2-5: Number of Access Classified by Source Area/Day in January 2010

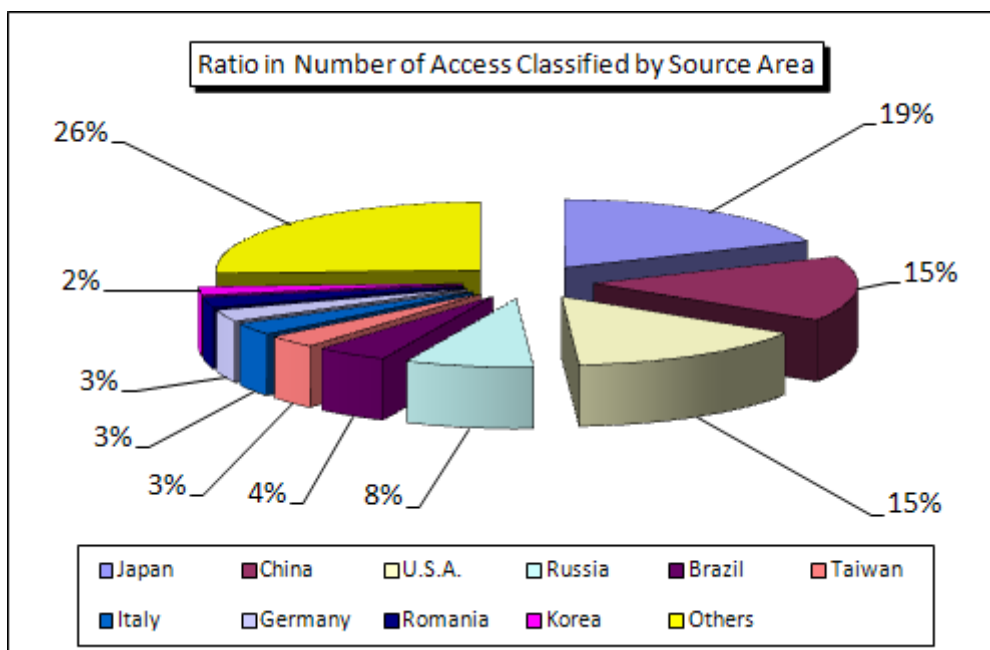


Chart 2-6: Ratio in Number of Access Classified by Source Area in January 2010

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 January 2010. 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.

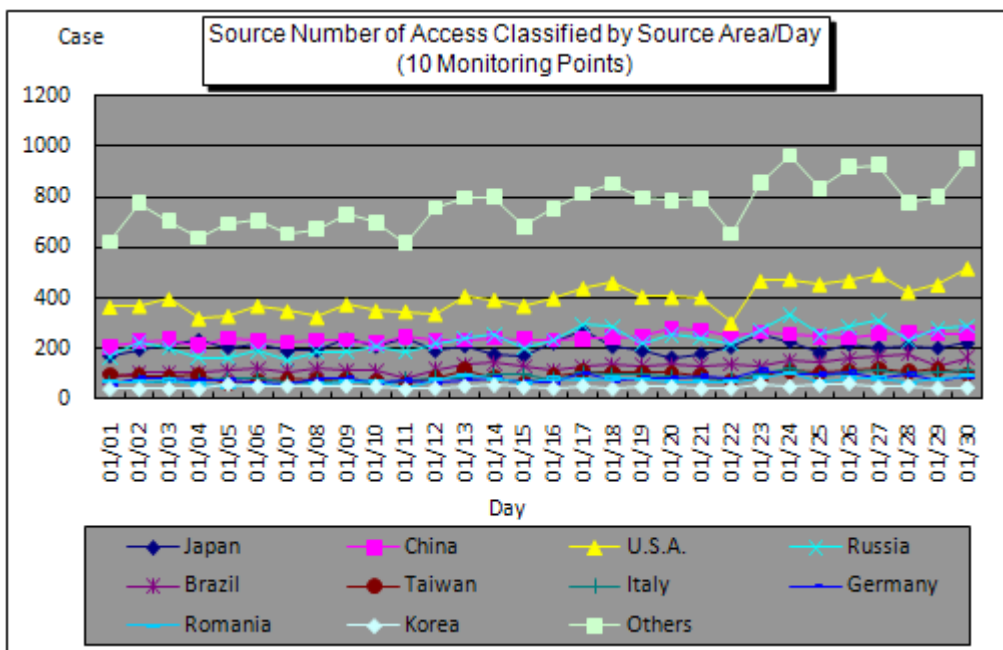


Chart 2-7: Source Number of Access Classified by Source Area/Day in January 2010

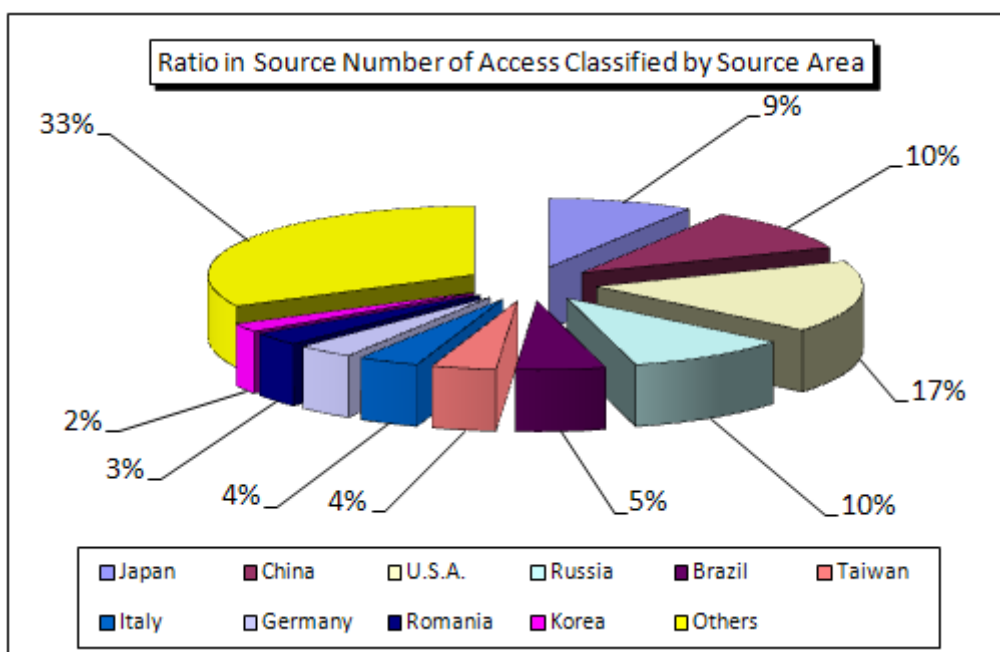


Chart 2-8: Ratio in Source Number of Access Classified by Source Area in January 2010

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 August 2009 to January 2010.

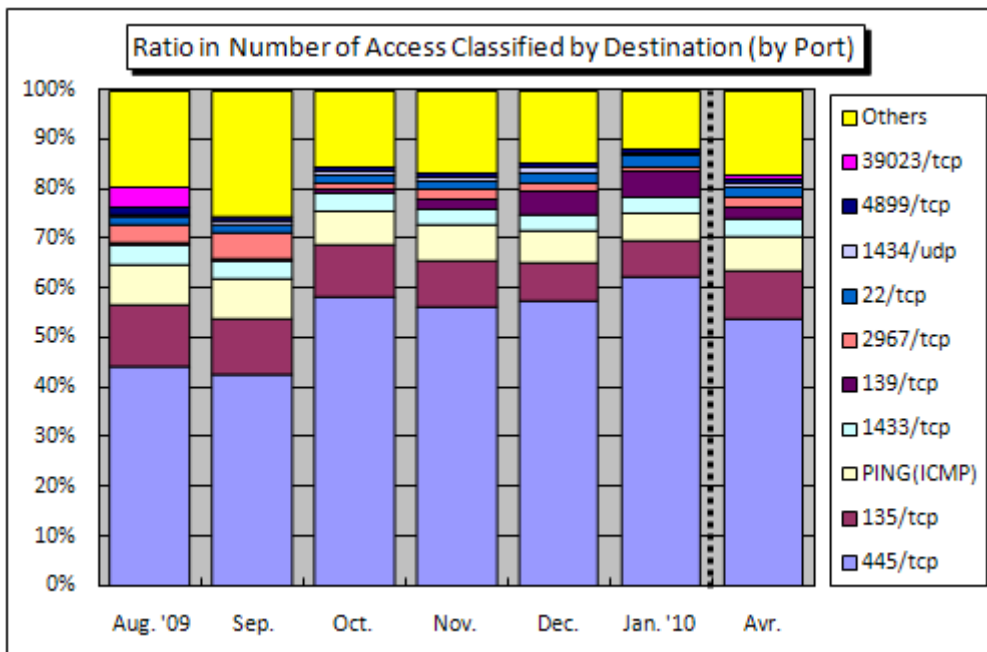


Chart 3-1: Ratio in Number of Access Classified by Destination (by Port) from August '09 to January '10

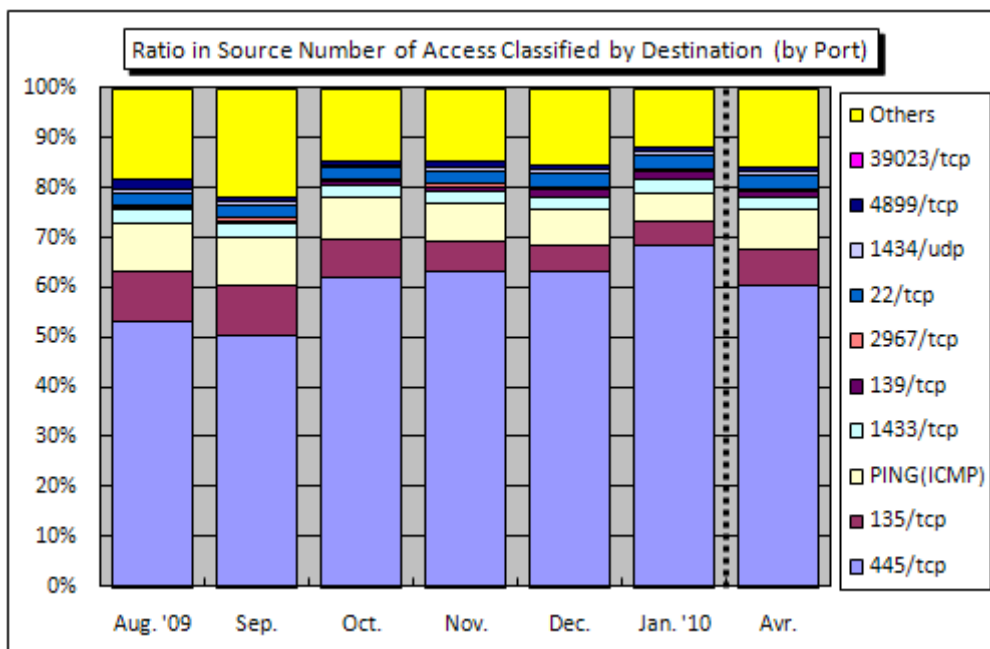


Chart 3-2: Ratio in Source Number of Access Classified by Destination (by Port) from August '09 to January '10

(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 August '09 to January 2010.

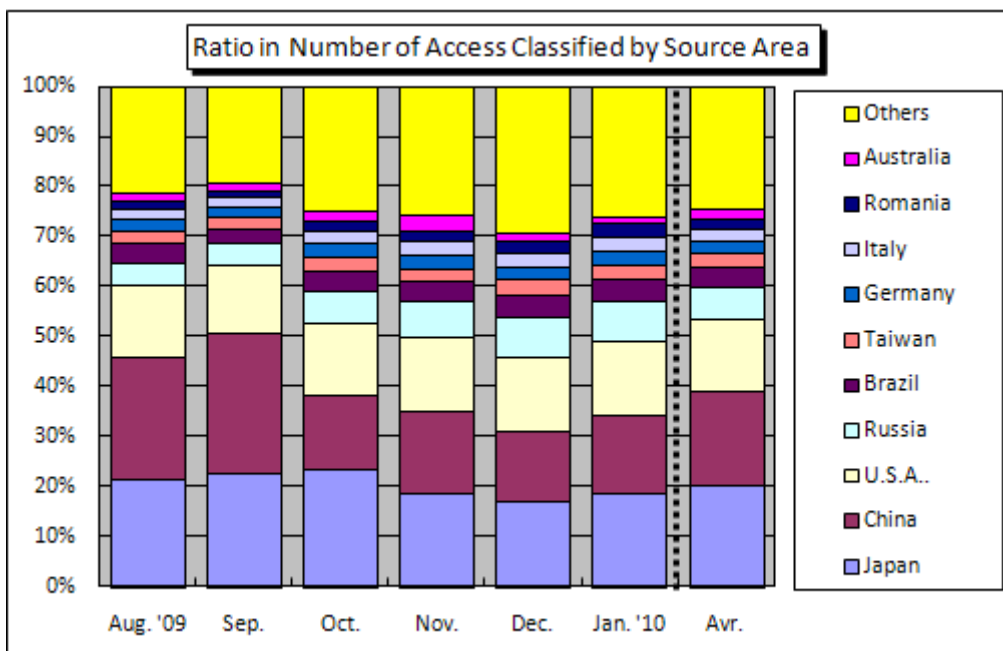


Chart 3-3: Ratio in Number of Access Classified by Source Area from August '09 to January '10

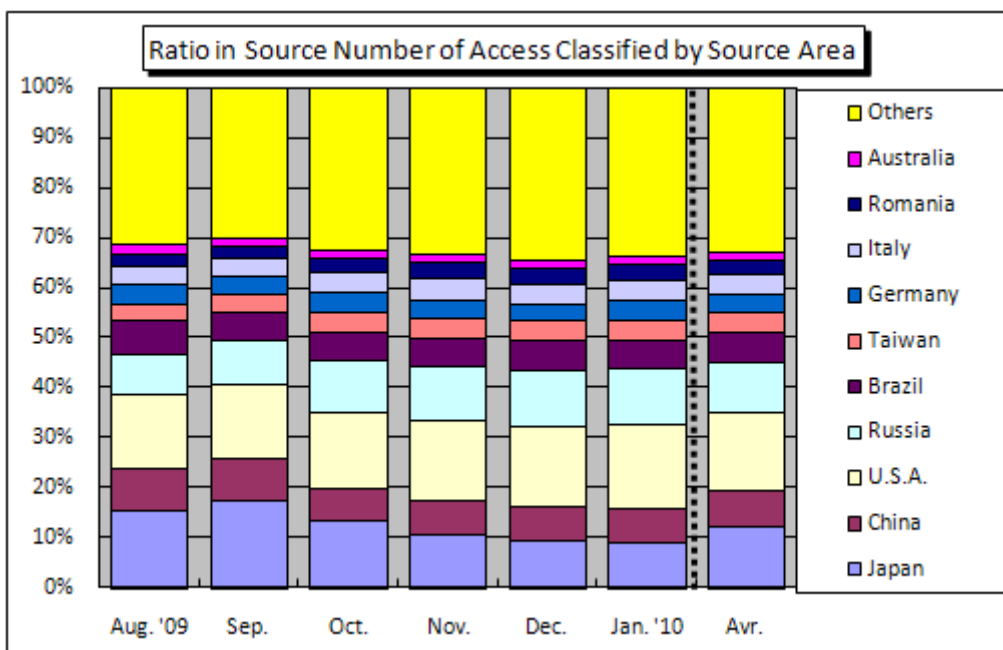


Chart 3-4: Ratio in Source Number of Access Classified by Source Area from Aug. '09 to Jan. '10

4. Supplementary Explanations

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in January 2010.

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.
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.
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.
1434/tcp	Renowned by unauthorized computer access targeting the vulnerability (by W32/SQL Slammer) in Microsoft SQL Server, etc.
5900/tcp	This access is highly probable which targets vulnerability in RealVNC, the one of remote accessing tools.
4899/tcp	Renowned by unauthorized access targeting the vulnerability in RAdmin (RAdmin is the one of applications that can operate several computers remotely).

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