

Report from the Internet Monitoring (TALOT2)

March 2009

1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in January totaled **136,473** cases for the 10 monitoring points and the gross number of the sources* was **44,646**: unwanted (one-sided) access captured at one monitoring point was about **440** accesses from about **144** sources per day.

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.

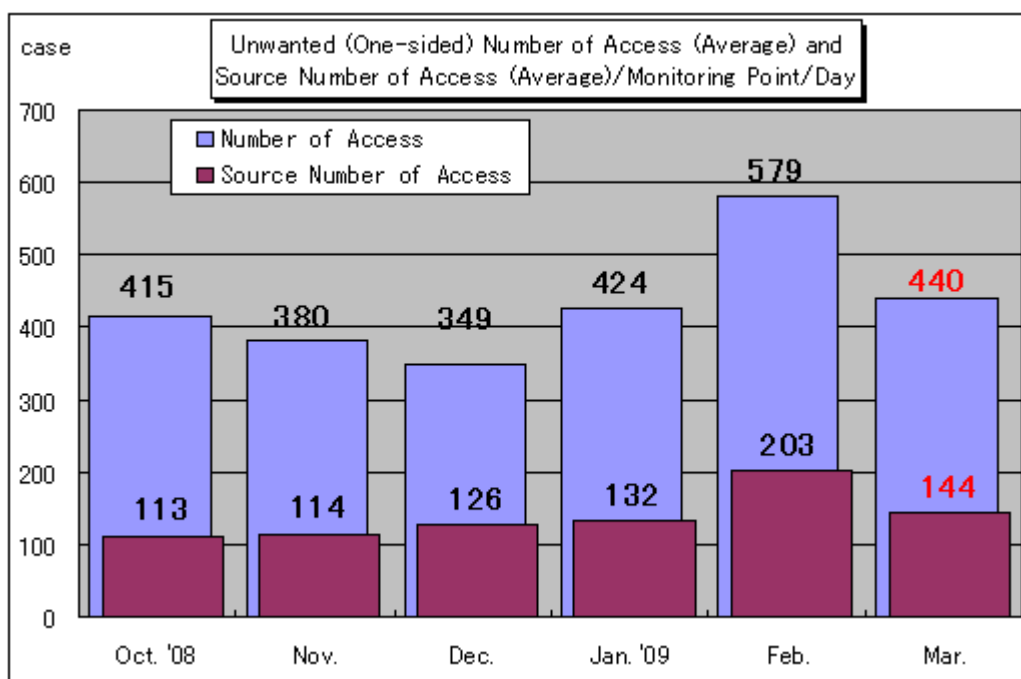


Chart 1-1: Unwanted (One-sided) Number of Access (Average) and Source Number of Access (Average)/Monitoring Point/Day

The Chart 1-1 shows that the number of access (average) and the source number of access (average)/monitoring point/day from October 2008 to March 2009. Both unwanted number of accesses (average) were drastically decreased from February.

The Chart 1-2 shows the number of access classified by destination (port type) in comparison with February. The one drastically decreased was the access to the port 445/tcp: decreased about 20,000 (February: about -56%). Please also refer to the (1) of Section 2 for further details. This is one of the high potential ports to be attacked when the vulnerability of Windows is targeted.

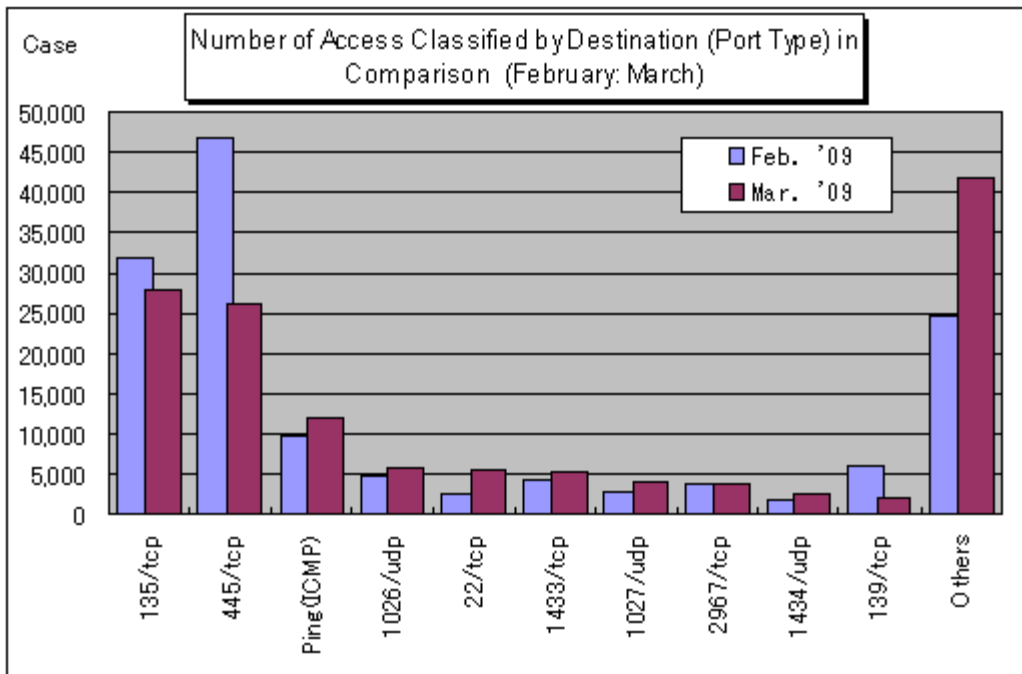


Chart 1-2: Number of Access Classified by Destination (Port Type) in Comparison (February: March)

2. The Peculiar Access in March 2009

(1) Access to the Port 445/tcp

It seemed that the access to the port 445/tcp was drastically decreased from the one in February: however, looking back to the previous year, the access to the port 445/tcp was indeed, remarkable in February, but in March, the access to the port 445/tcp was only gotten back to the standard (See the Chart 2-1). The timing for the access increase to the port 445/tcp in February was system stoppage relevant to the TALOT2 maintenance activities, and the timing for the access decrease to this port in March was caused by changing TALOT2 monitoring points which conducted irregularly. The essential causes for drastic access increase/decrease to the port 445/tcp in respective timings are not yet identified.

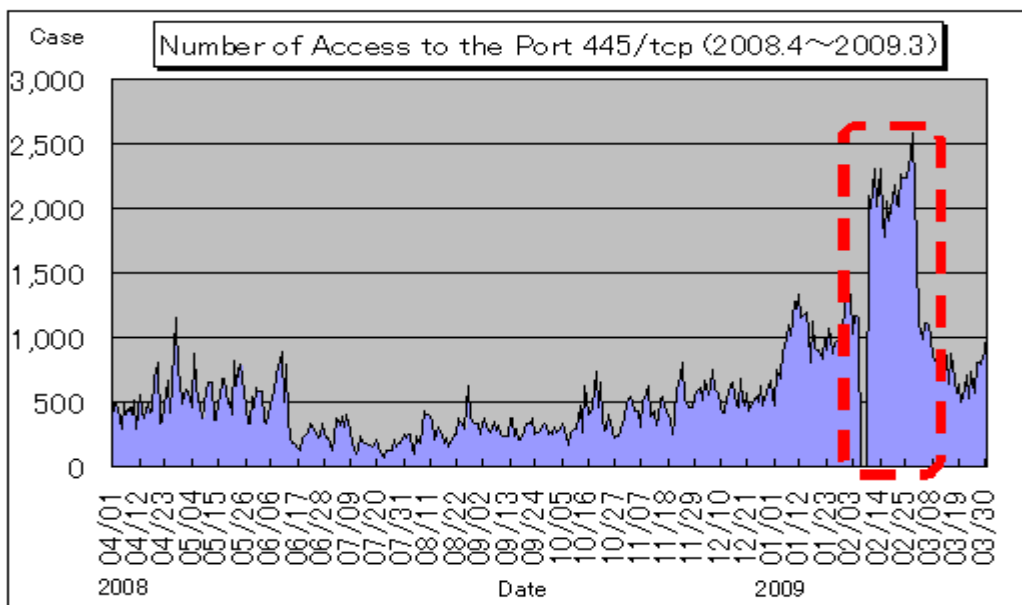


Chart 2-1: Shift in Number of Access to the Port 445/tcp Classified by Source Area

3. One-sided Access in March 2009

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

The Chart 3-1 shows the shift in unwanted (one-sided) accessing status (number of access) and the Chart 3-2 shows the shift in unwanted (one-sided) accessing status (source number of access) in March 2009.

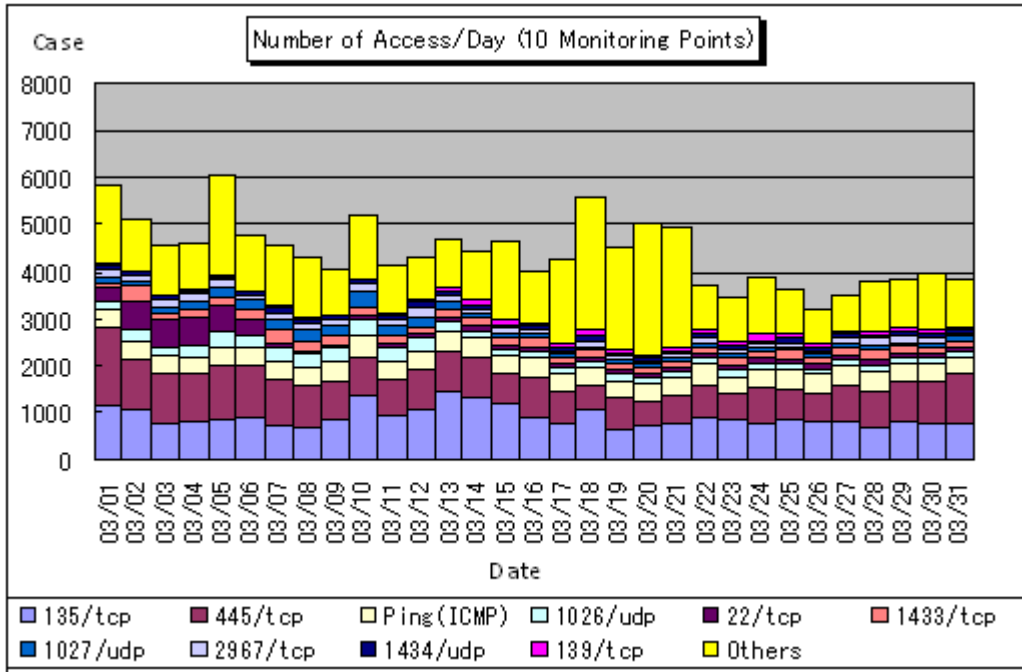


Chart 3-1: Shift in Number of Access/Day in March 2009

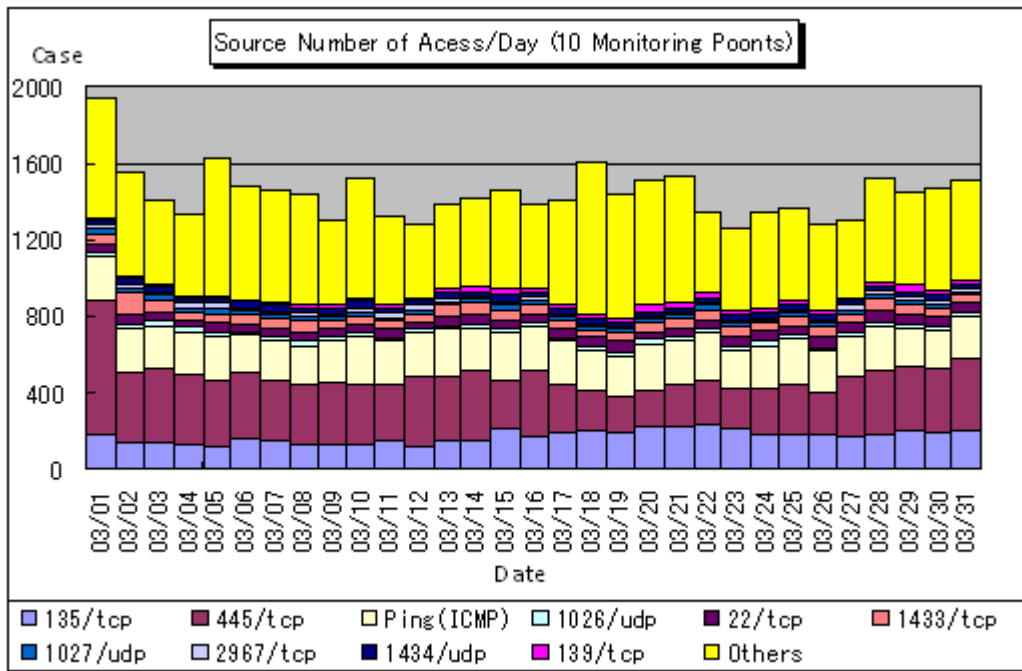


Chart 3-2: Shift in Source Number of Access/Day in March 2009

(2) Ratio Classified by Destination (Port Type)

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

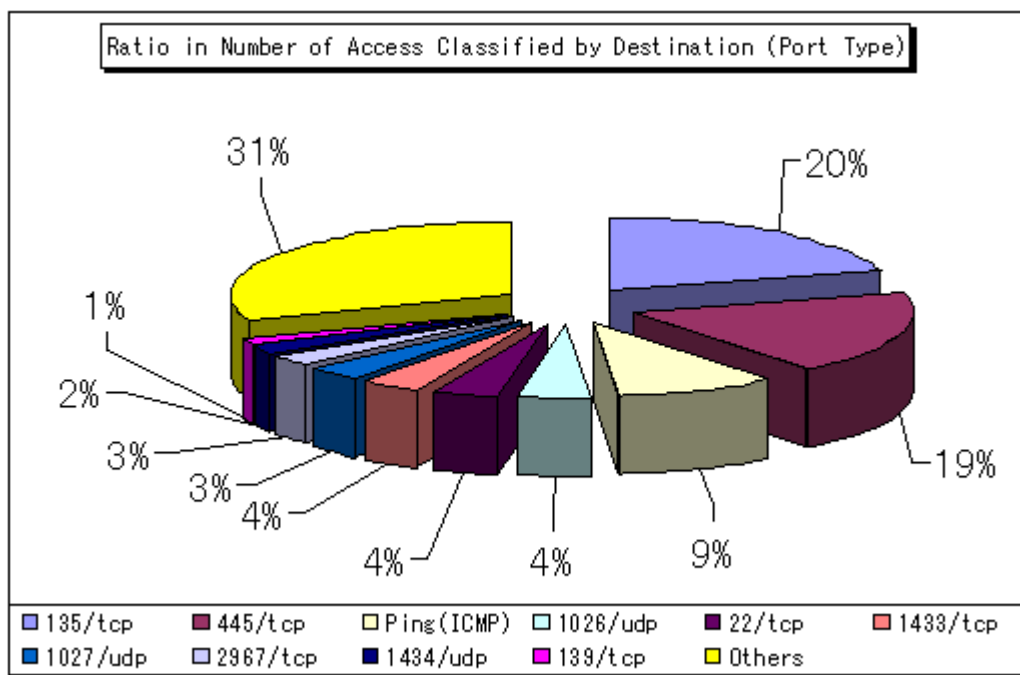


Chart 3-3: Ratio in Number of Access Classified by Destination (Port Type) in March 2009

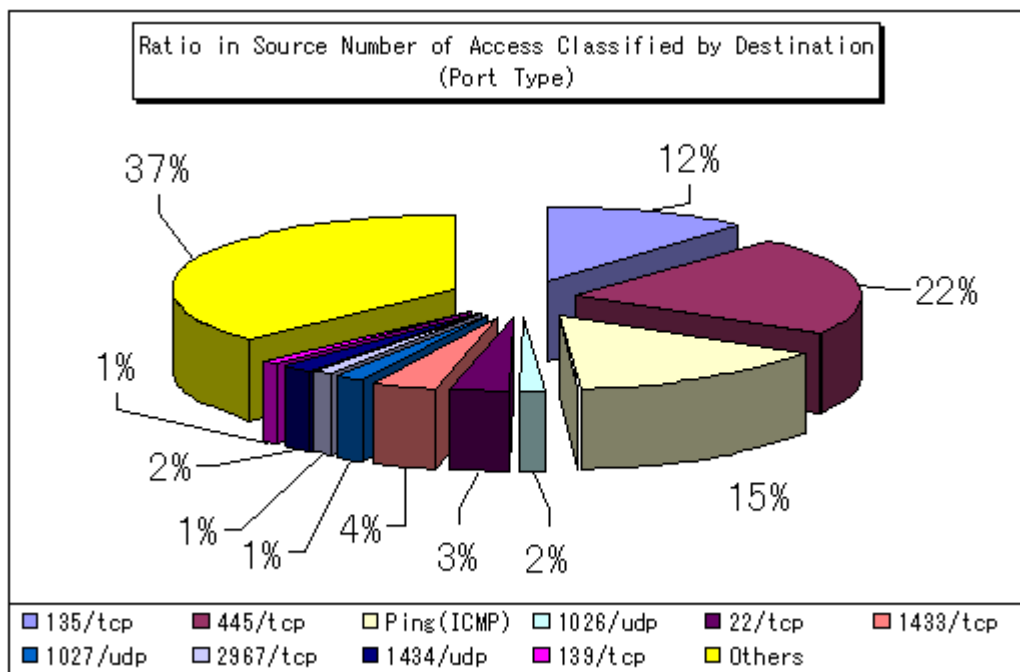


Chart 3-4: Ratio in Source Number of Access Classified by Destination (Port Type) in March 2009

(3) Accessing Status Classified by Source Area

The Chart 3-5 shows the shift in number of access classified by source area and the Chart 3-6 shows the ratio in number of access classified by source area in March 2009. For your information, each ratio is rounded at the 1st arithmetic point so that the total may not make 100% sharp, accordingly.

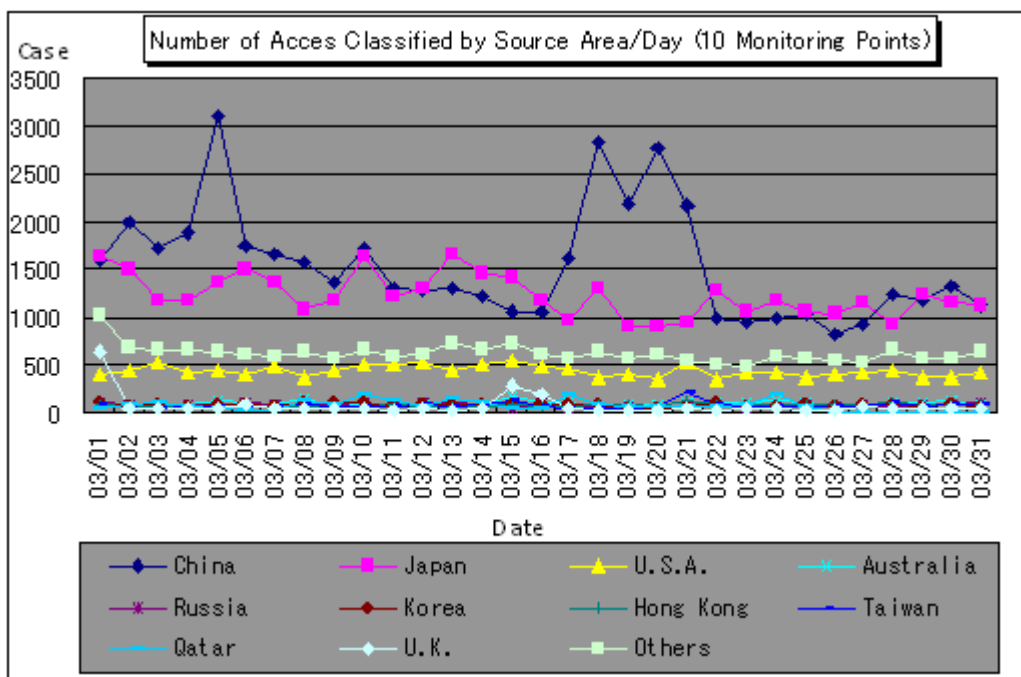


Chart 3-5: Shift in Number of Access/Day Classified by Source Area in March 2009

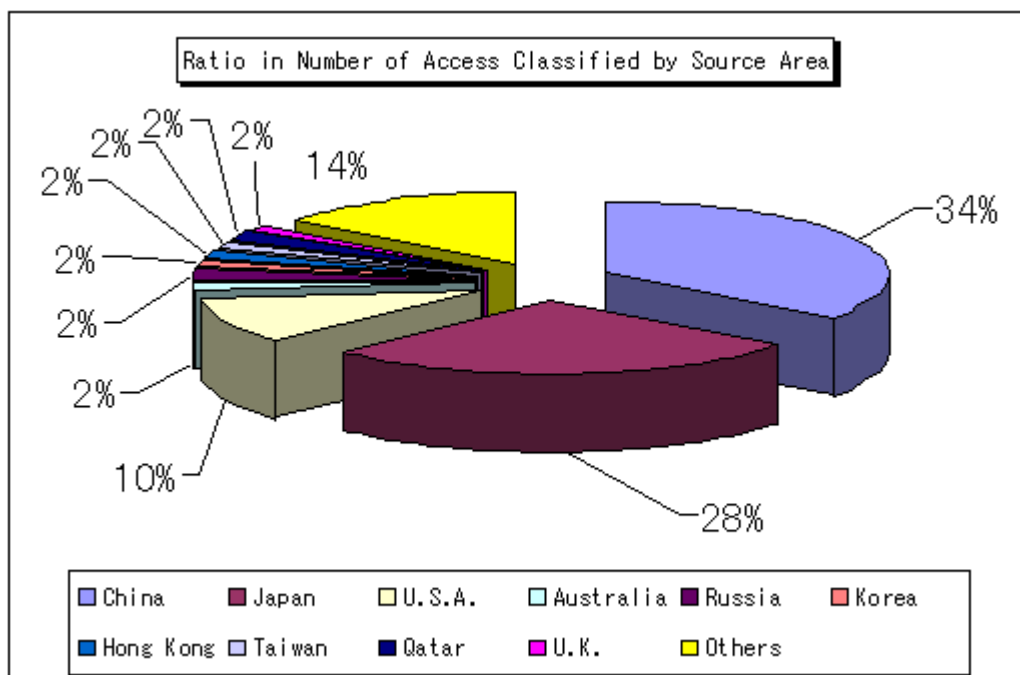


Chart 3-6: Ratio in Number of Access Classified by Source Area in March 2009

The Chart 3-7 shows the shift in source number of access classified by source area and the Chart 3-8 shows the ratio in source number of access classified by source area in March 2009. For your information, each ratio is rounded at the 1st arithmetic point so that the total may not make 100% sharp, accordingly.

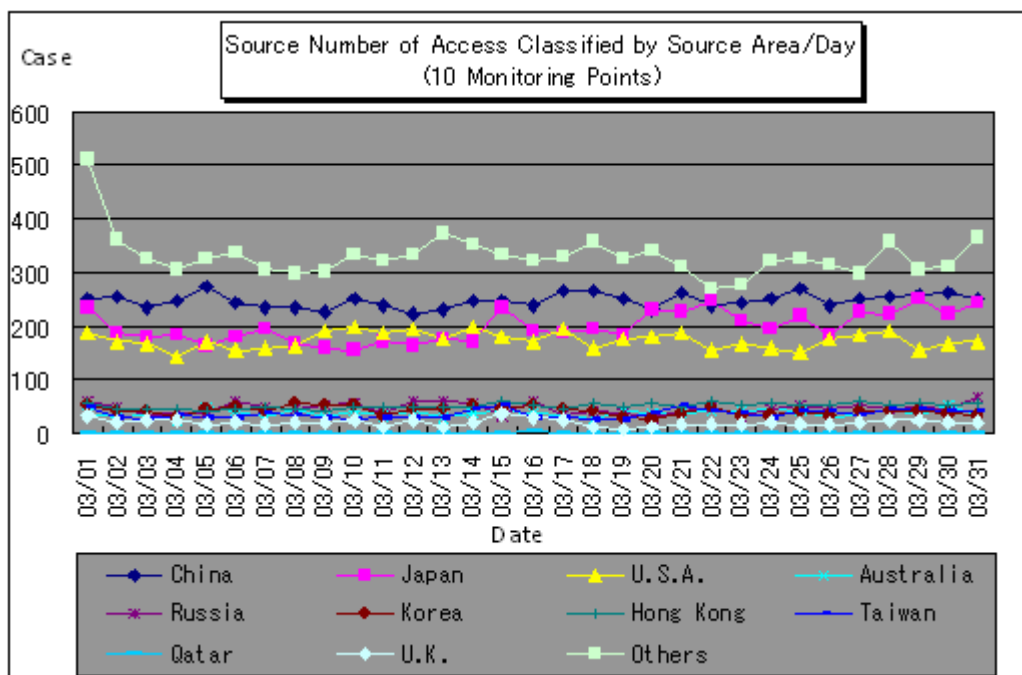


Chart 3-7: Shift in Source Number of Access Classified by Source Area/Day in March 2009

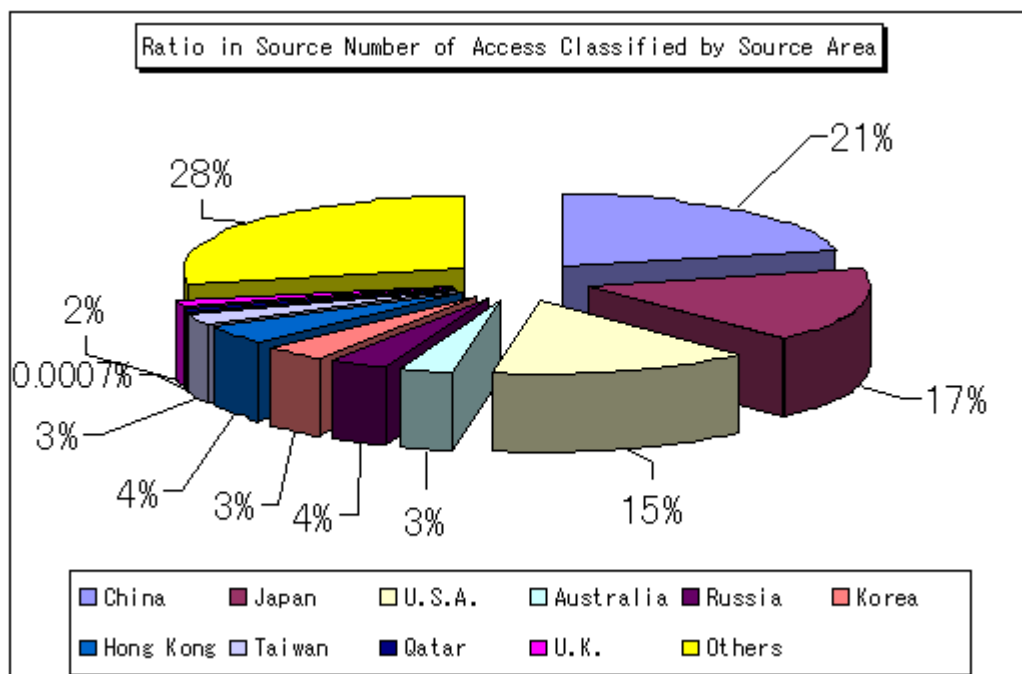


Chart 3-8: Ratio in Source Number of Access Classified by Source Area in March 2009

4. Statistical Information

(1) Ratio Classified by Destination (Port Type)

The Chart 4-1 shows the ratio in number of access classified by destination (port type) and the Chart 4-2 shows the ratio in source number of access classified by destination from October 2008 to March 2009.

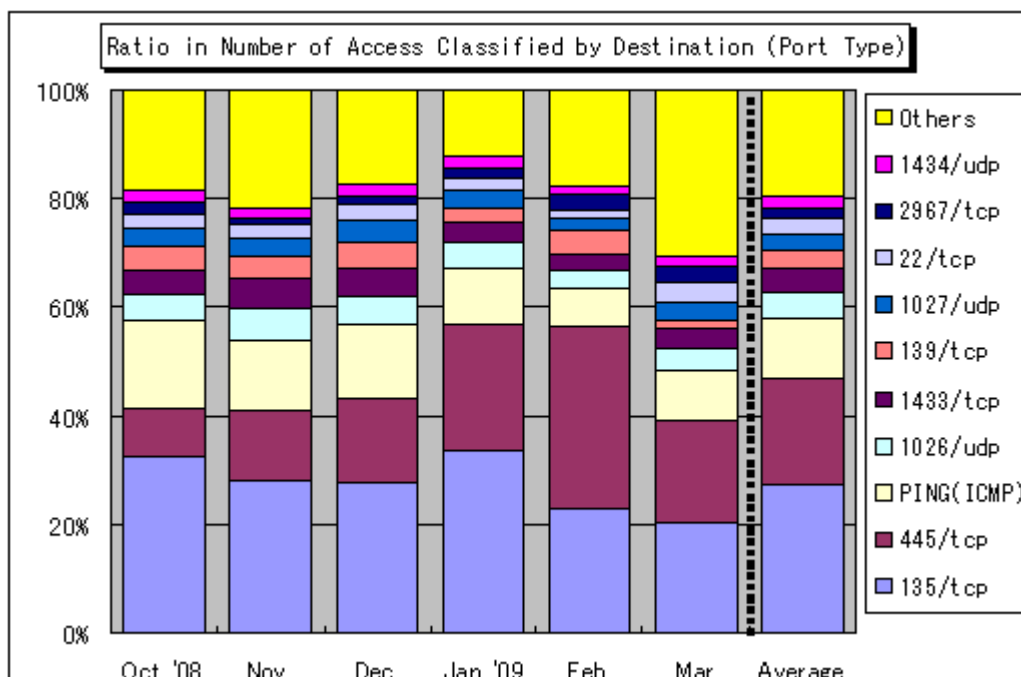


Chart 4-1: Ratio in Number of Access Classified by Destination (Port Type) from October 2008 to March 2009

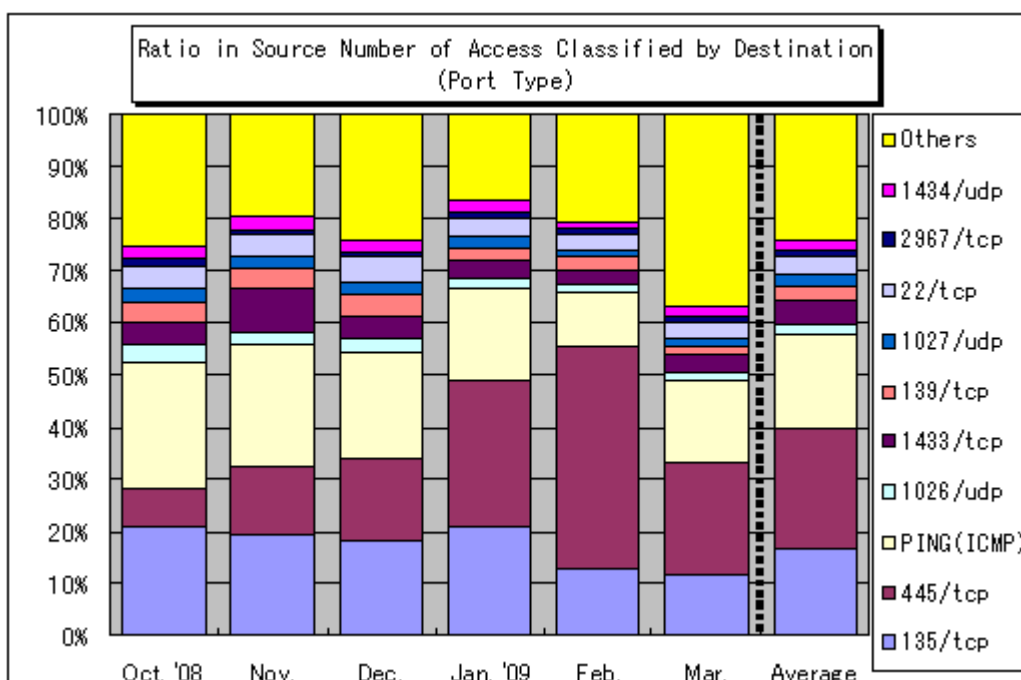


Chart 4-2: Ratio in Source Number of Access Classified by Destination (Port Type) from October 2008 to March 2009

(2) Ratio Classified by Destination

The Chart 4-3 shows the ratio in number of access classified by source area and the Chart 4-4 shows the ratio in source number of access classified by source area from October 2008 to March 2009.

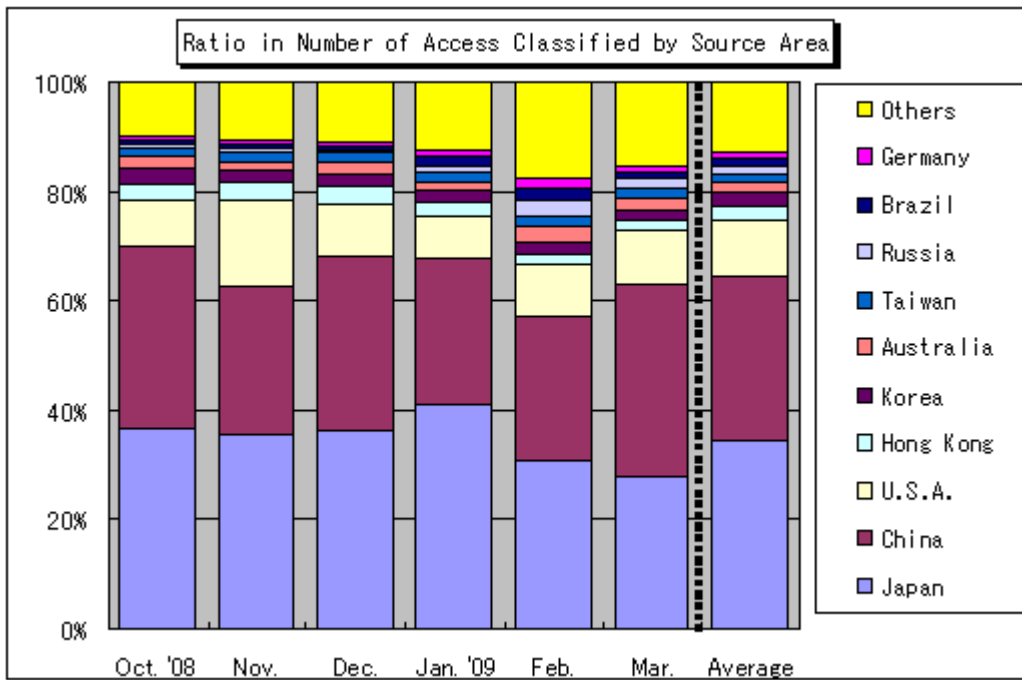


Chart 4-3: Ratio in Number of Access Classified by Source Area from October 2008 to March 2009

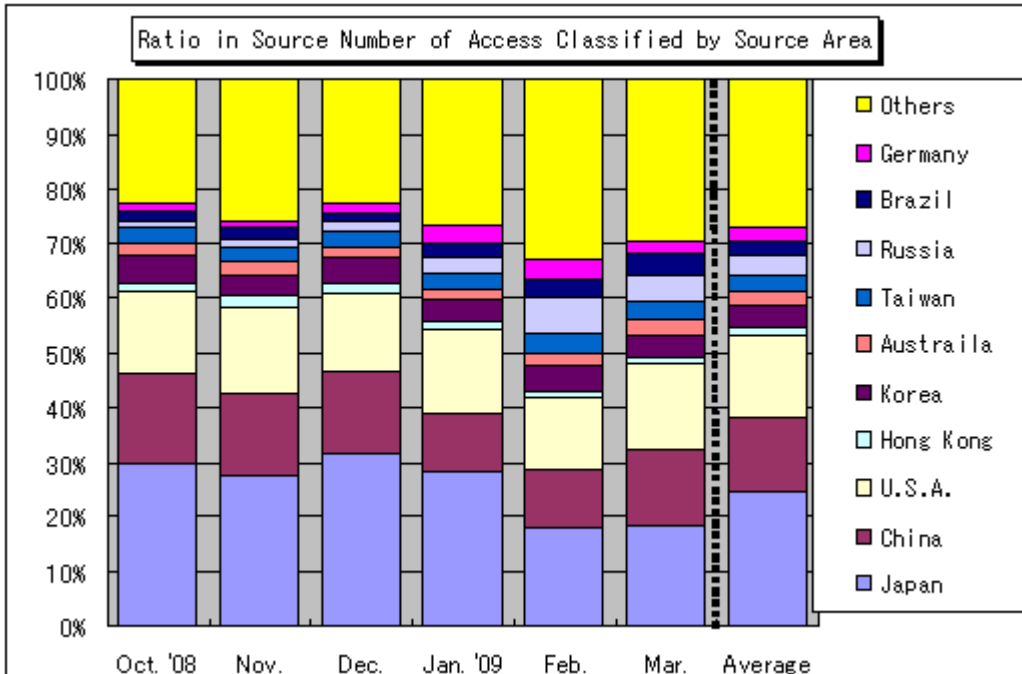


Chart 4-4: Ratio in Source Number of Access Classified by Source Area from October 2008 to March 2009

5. Supplementary Explanations

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in March 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.
139/tcp	Renowned to target those file sharing (network sharing) that has not been well-protected; generally, it is probable to be the accesses targeting vulnerabilities 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.
1026/udp, 1027/udp	Renowned for sending pop-up (spam) messages exploiting Microsoft Windows Messenger service which differs from MSN Messenger.
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 the fraudulent access, etc. targeting vulnerability in Microsoft SQL Server (W32/SQLSlammer, etc.).
2967/tcp	High potential of access which targets vulnerability in Symantec products.

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