

Report from the Internet Monitoring (TALOT2)

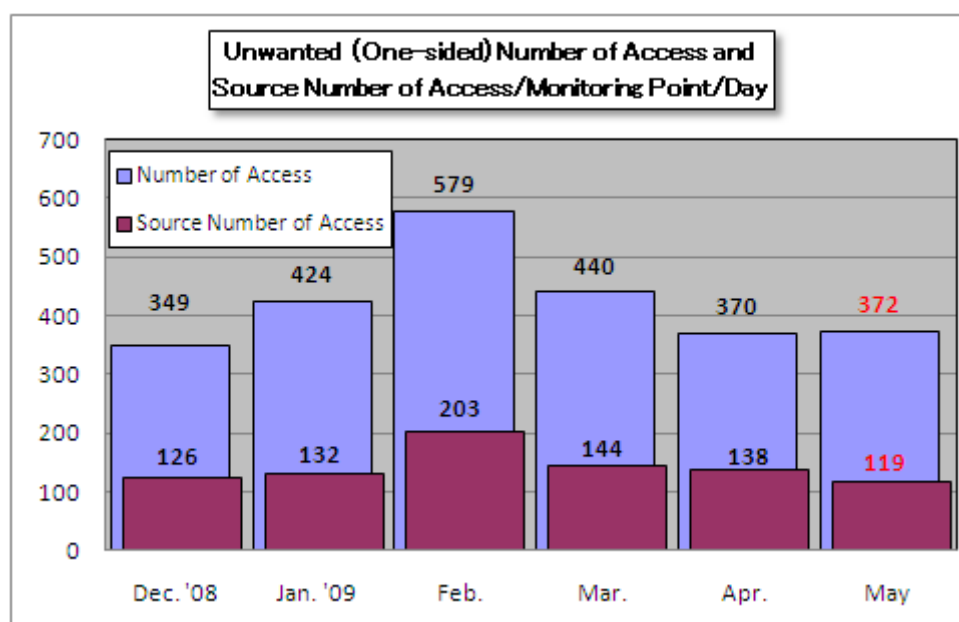
May 2009

1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in May totaled **115,336** cases for the 10 monitoring points and the gross number of the sources* was **36,779**: unwanted (one-sided) access captured at one monitoring point was about **372** accesses from about **119** 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 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 from December 2008 to May 2009. Both the unwanted (one-sided) number of accesses were shifted in almost same level.

The Chart 1-2 shows the comparison in number of access for April and May classified by destination (by port). In May, significant increase/decrease in the number of access was not monitored. However, accesses to the ports 11245/tcp and 11245/udp for which never monitored in April were drastically increased in May.

The cause of such access increase to these ports was intensively accessed to one of the monitoring points for TALOT2 from Specific source address in the first half of May. The cause of such intensive access has not yet identified.

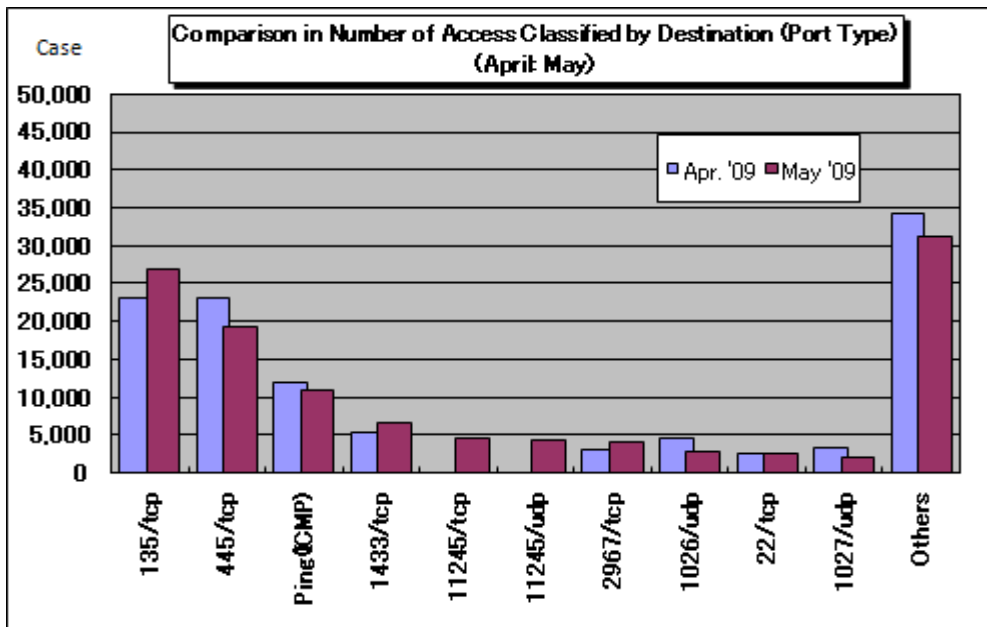


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (April: May)

2. Peculiar Access in May 2009

(1) Access to the Port 2967/tcp

The Chart 2-1 shows that the access to the port 2967/tcp tended to increase in the early part of May.

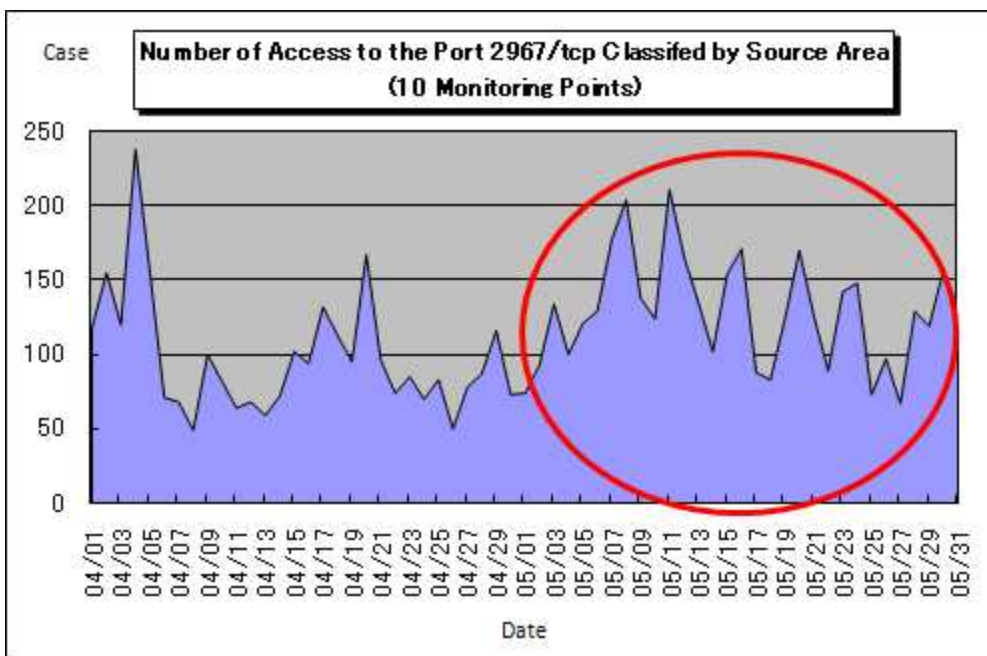


Chart 2-1: Number of Access to the Port 2967/tcp (10 Monitoring Points Total)

The Port 2967/tcp is the default port exclusively used by Symantec products. As for the vulnerability in the port likely to be exploited by attacks, "Vulnerability in Symantec Client Security and Symantec AntiVirus Allows Privilege Escalation (SYM06-010)" was publicized in the past.

This vulnerability allows attacker to fraudulently acquire/delete files such as Symantec Client Security and Symantec AntiVirus, etc. so that the system is likely to be crushed.

<Reference>

"Symantec Client Security and Symantec AntiVirus Elevation of Privilege (SYM06-010)"
<http://www.symantec.com/avcenter/security/Content/2006.05.25.html>

Accordingly, if the vulnerability in the said products is not resolved, you will likely be attacked by exploiting that vulnerability. To prevent yourself from damage, it is important to be cautious with the information relevant to vulnerability: when information relevant to your products is publicized, be sure to resolve them in your earliest convenience.

For your information, the homepages provided by the vendor for the products you are now using and the portal site for vulnerability information such as JVN are very much helpful: accordingly, be sure to check them periodically to be ready to conduct necessary anti-vulnerability measures on time.

<Reference>

"JVN (Japan Vulnerability Notes)" (portal site for vulnerability information) (in Japanese)
<http://jvn.jp/>

"JVN iPedia - Information database for anti-vulnerability measures information" (in Japanese)
<http://jvndb.jvn.jp/>

3. Status for Unwanted (One-sided) Number of Access in May

(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).

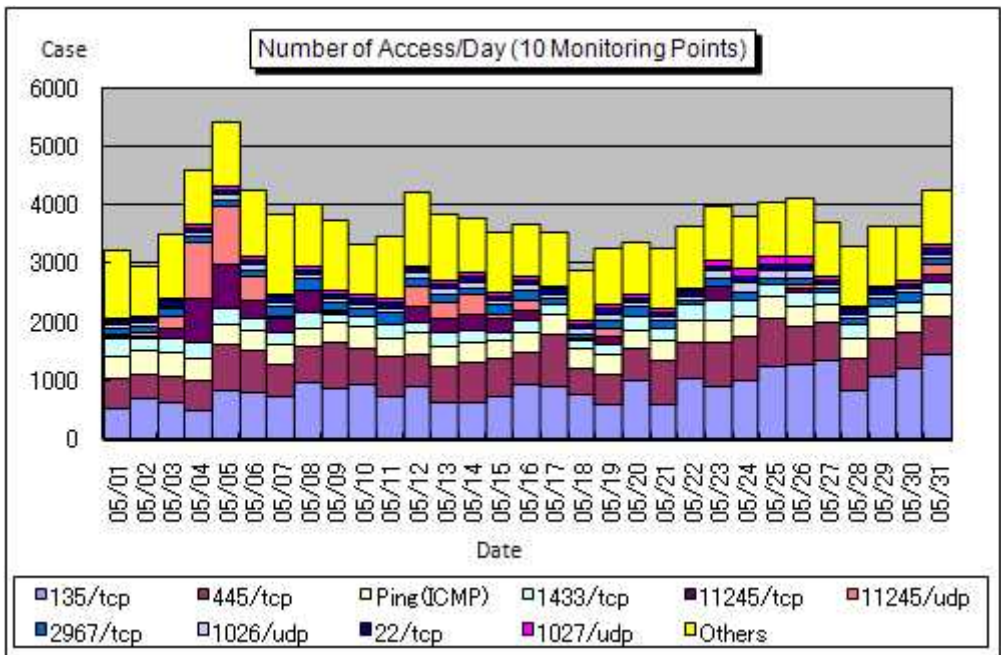


Chart 3-1: Number of Access/Day in May 2009

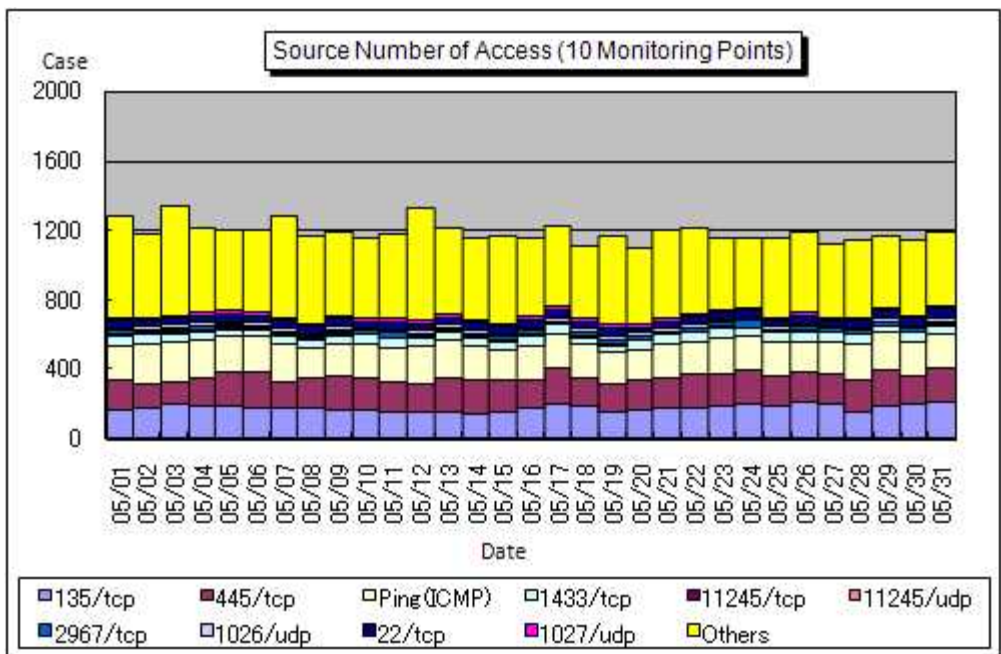


Chart 3-2: Source Number of Access/Day in May 2009

(2) Ratio Classified by Destination (Port Type)

The Chart 3-3 shows the ratio in unwanted (one-sided) number of access classified by destination and the Chart 3-4 shows the ratio in unwanted (one-sided) source number of access classified by destination. For your information, ratios are rounded at the 1st arithmetic point so that they may not make 100% sharp, accordingly.

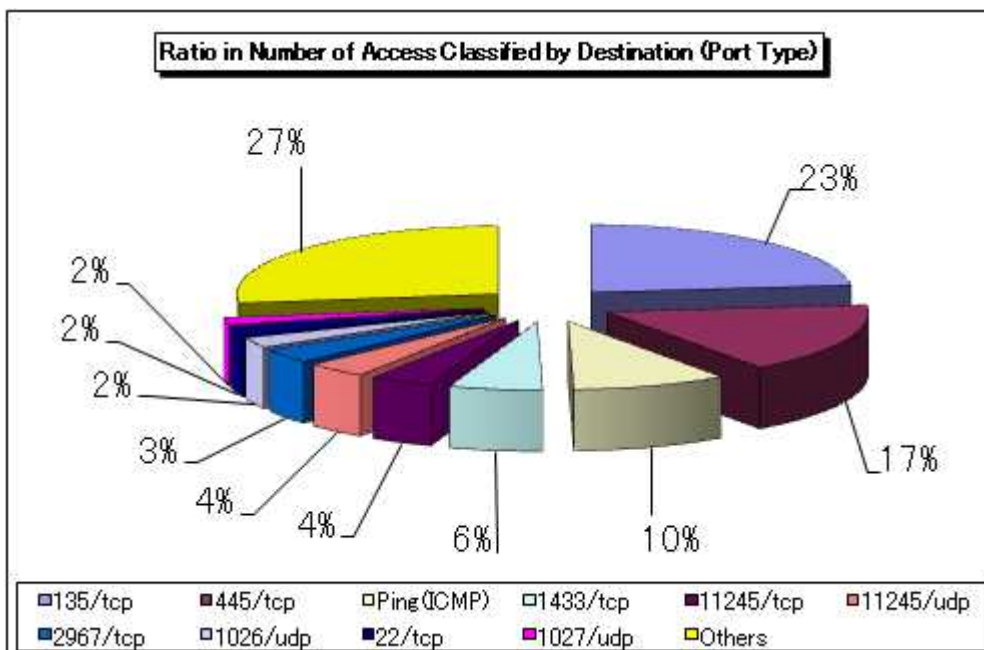


Chart 3-3: Ratio in Number of Access Classified by Destination (Port Type) in May 2009

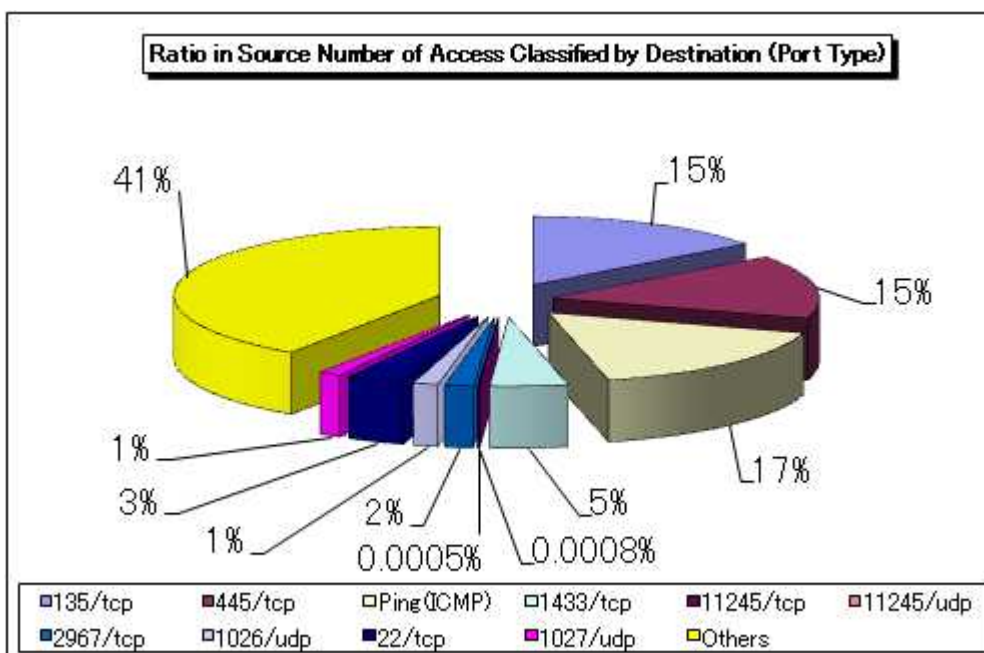


Chart 3-4: Ratio in Source Number of Access Classified by Destination (Port Type) in May 2009

(3) Accessing Status Classified by Source Area

The Chart 3-5 shows the shift in unwanted (one-sided) number of access and the Chart 3-6 shows the ratio in unwanted (one-sided) number of access classified by source area. For your information, ratios are rounded at the 1st place of arithmetic point so that they not make 100% sharp, accordingly.

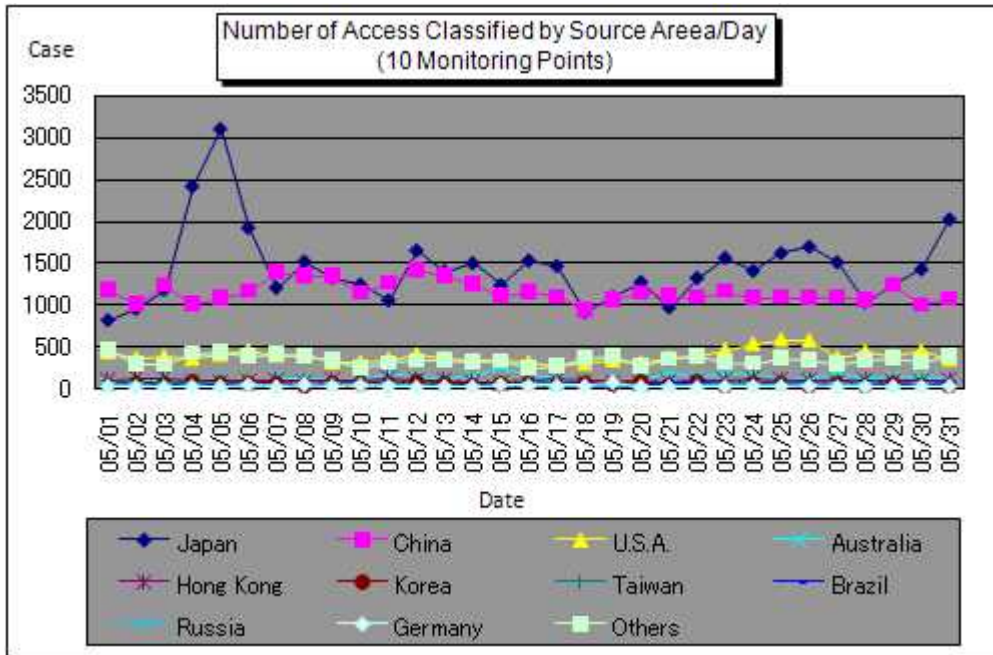


Chart 3-5: Number of Access Classified by Source Area/Day in May 2009

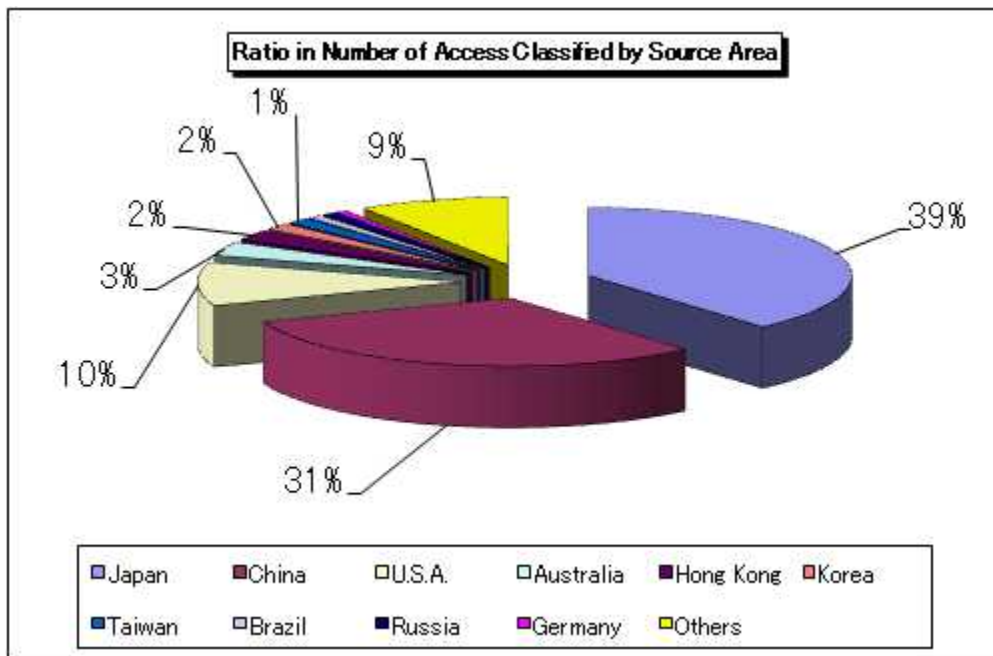


Chart 3-6: Ratio in Number of Access Classified by Source Area in May 2009

The Chart 3-7 shows the shift in unwanted (one-sided) 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 May 2009. For your information, ratios are rounded at the 1st arithmetic point so that they not make 100% sharp, accordingly.

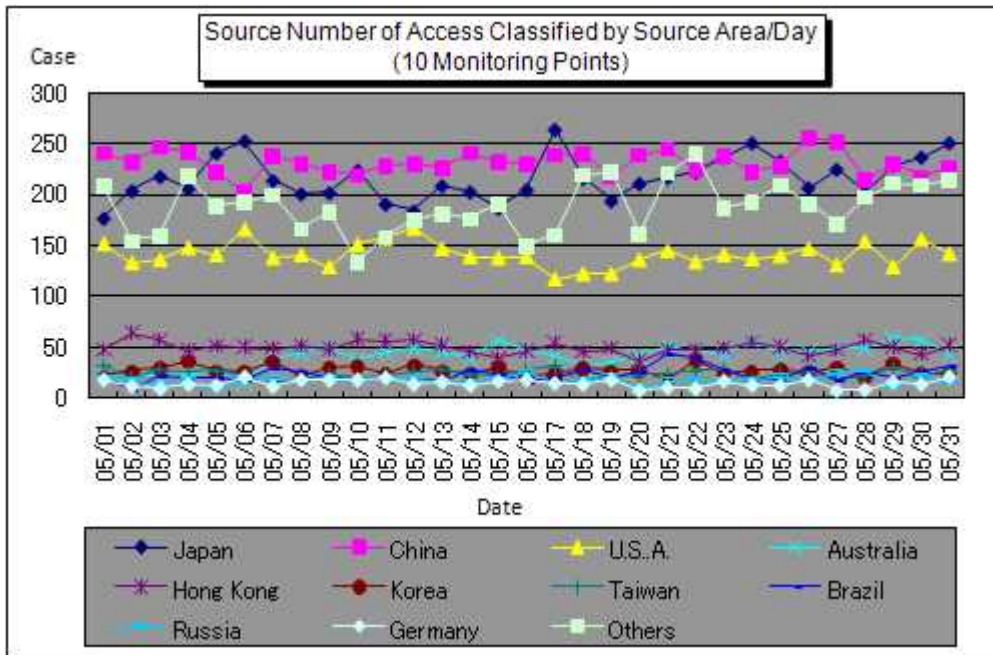


Chart 3-7: Source Number of Access Classified by Source Area/Day in May 2009

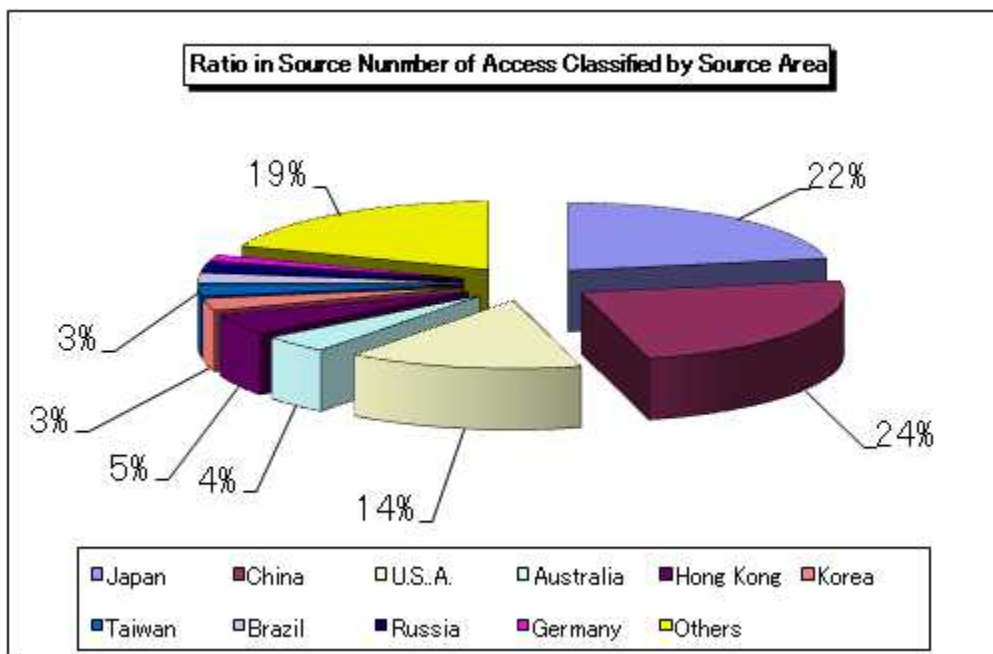


Chart 3-8: Ratio in Source Number of Access Classified by Source Area in May 2009

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 (port type) from December 2008 to May 2009.

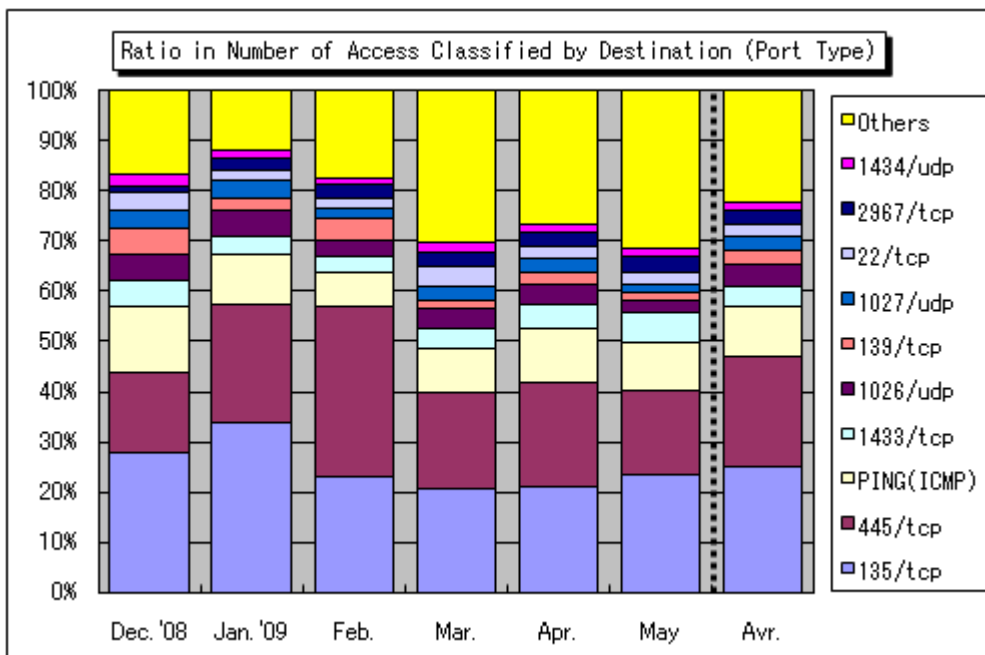


Chart 4-1: Ratio in Number of Access Classified by Destination (Port Type) from December 2008 to May 2009

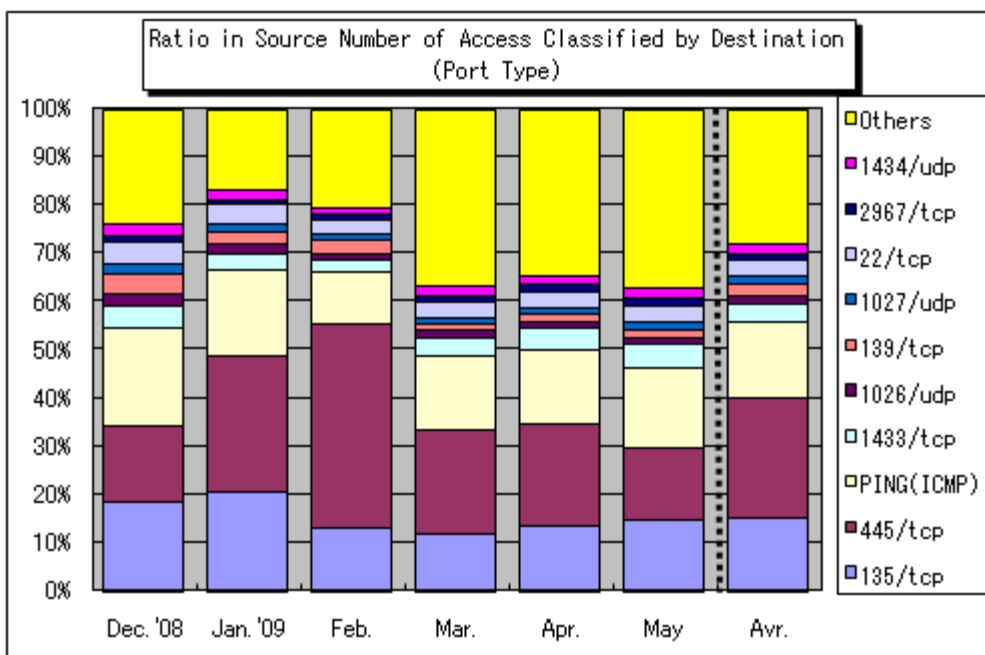


Chart 4-2: Ratio in Source Number of Access Classified by Destination (Port Type) from December 2008 to May 2009

(2) Ratio Classified by Source Area

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 December 2008 to May 2009.

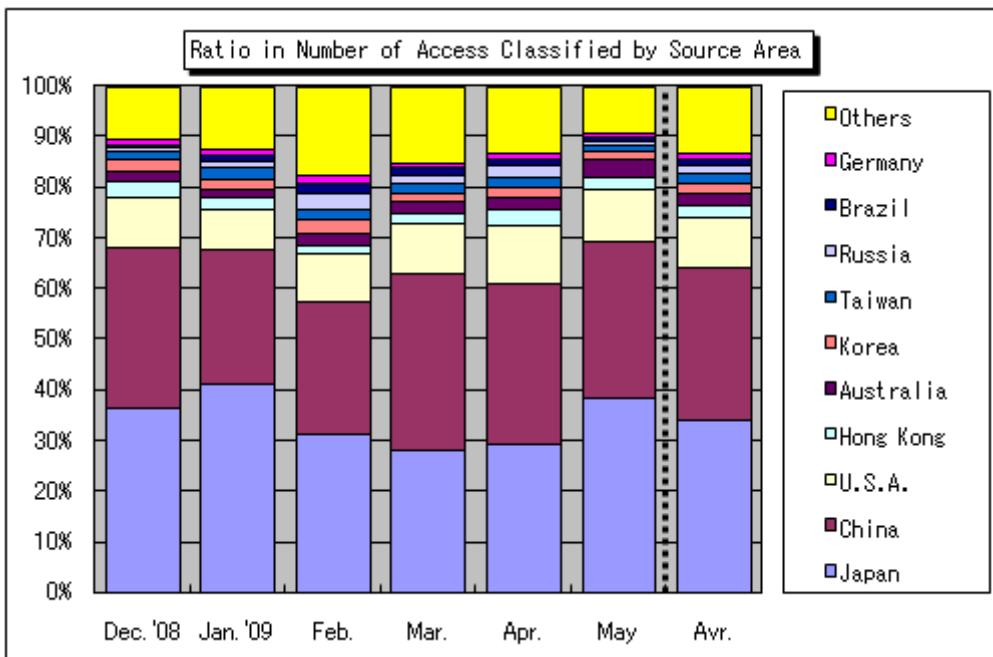


Chart 4-3: Ratio in Number of Access Classified by Source Area from December 2008 to May 2009

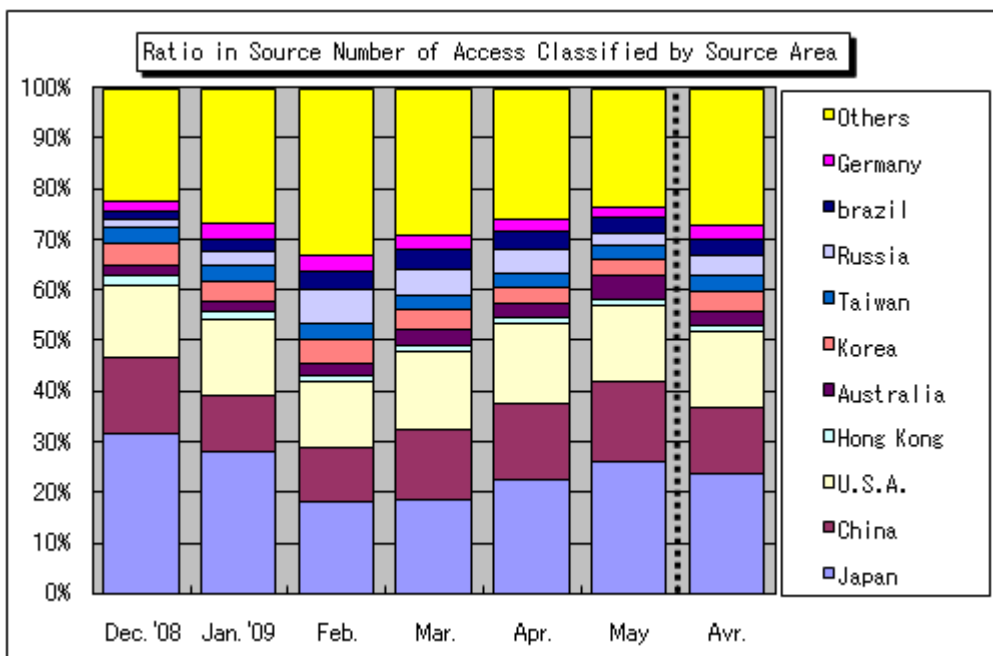


Chart 4-4: Ratio in Source Number of Access Classified by Source Area from December 2008 to May 2009

5. Supplementary Descriptions

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in May 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.
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.
2967/tcp	High potential of access which targets vulnerability in Symantec products.
11245/tcp, 11245/udp	They are the accesses from specific source area only monitored by one monitoring point for which cause is unknown.

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