Attachment 3

Observation by Internet Fix-Point Monitoring System (TALOT2) for July 2011

1. To General Internet Users

According to the Internet Fixed-Point Monitoring System (TALOT2), **102,888** unwanted (one-sided) accesses were observed at ten monitoring points in July 2011 and the total number of sources* was **46,222**. This means on average, **343 accesses** form **154 sources** were observed at **one monitoring point per day**. (See Figure 1-1)

*Total number of sources: indicates how many sources in total were observed by TALOT2. If multiple accesses from the same source were observed at the same monitoring point/port on the same day, they are considered one access from the specific source on that day.

Since the environment of each monitoring point for TALOT2 is equivalent to that of general Internet connection, an equal number of such accesses are thought to be made in the Internet users' system environment.

* For maintenance work, we shut down the systems on July 2. Therefore, the statistical information was derived from the data excluding that of July 2. Normally, the systems are in operation all times.

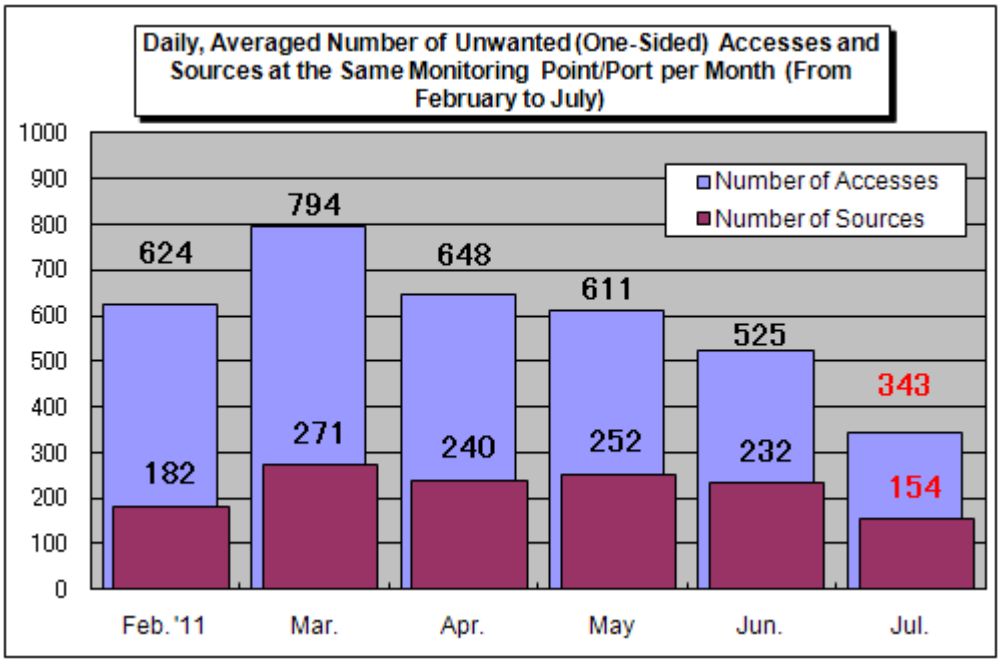

Figure1-1: Daily, Averaged Number of Unwanted (One-Sided) Accesses and Sources at the Same Monitoring Point/Port per Month (February 2011 to July 2011)

The Figure 1-1 shows daily, averaged number of unwanted (one-sided) accesses and sources at the same monitoring point/port per month (from February 2011 to July 2011). As shown in this figure, the number of unwanted (one-sided) accesses in July has decreased significantly, compared to the July level.

The Figure 1-2 shows the July-over-July comparison results for the number of unwanted (one-sided) accesses, classified by destination (port type). As shown in this figure, compared to the July level, access to 445/tcp has decreased significantly while access to 11083/tcp has increased.

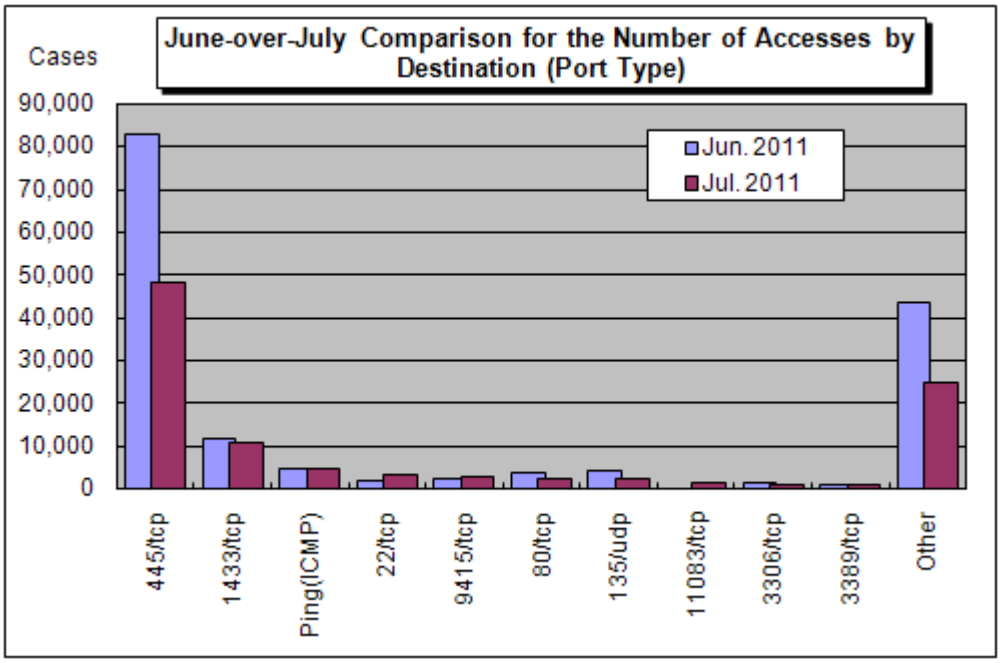

Figure 1-2: July-over-June Comparison for the Number of Accesses by Destination (Port Type)

Access to 11083/tcp began to be observed at a single monitoring point for TALOT2 after July 3 and such access was mainly made from the U.S and China (See Figure 1-3). It has yet to be identified why this port was accessed as it is not the one used by a specific application.

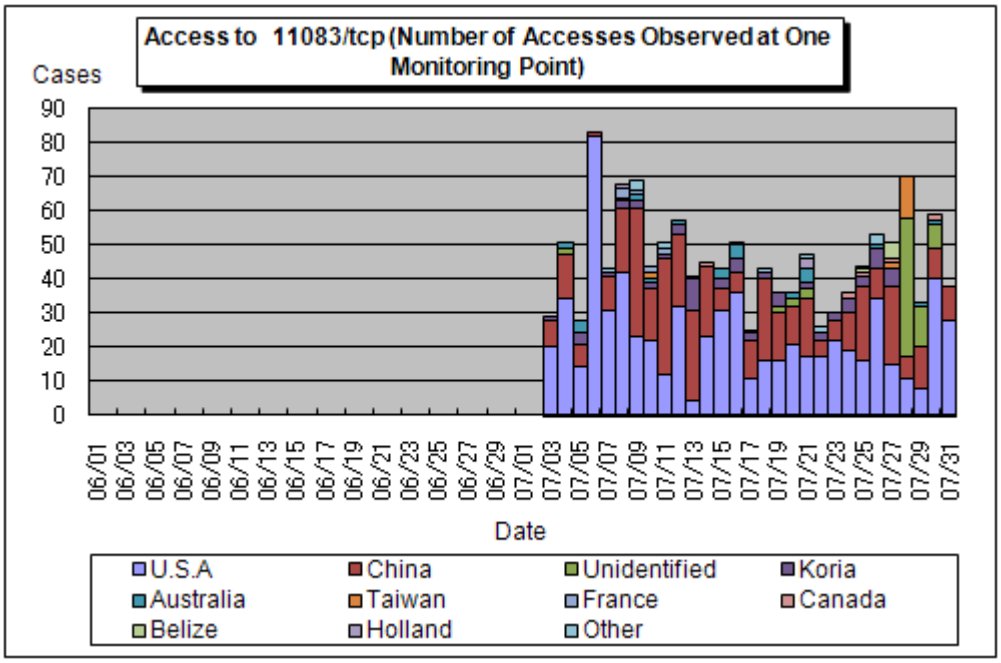

Figure 1-3: Access to 11083/tcp (Total Number of Accesses Observed at a Single Monitoring Point)

2. Unwanted(One-Sided) Access Observed in July 2011

(1) Unwanted(One-Sided) Access Observed, Segmented By Destination (Port Type)

Figure 2-1 shows the day-by-day variation in the number of unwanted (one-sided) accesses observed in July 2011. Figure 2-2 shows the day-by-day variation in the number of sources.

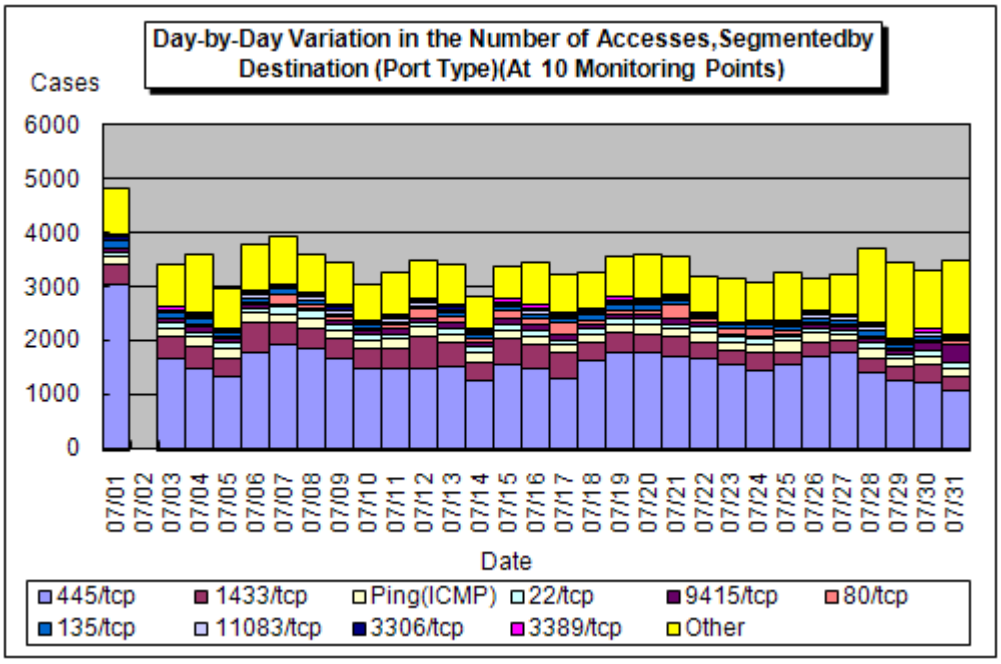

Figure2-1: Day-by-Day Variation in the Number of Accesses, Segmented by Destination (Port Type)(At 10 Monitoring Points)

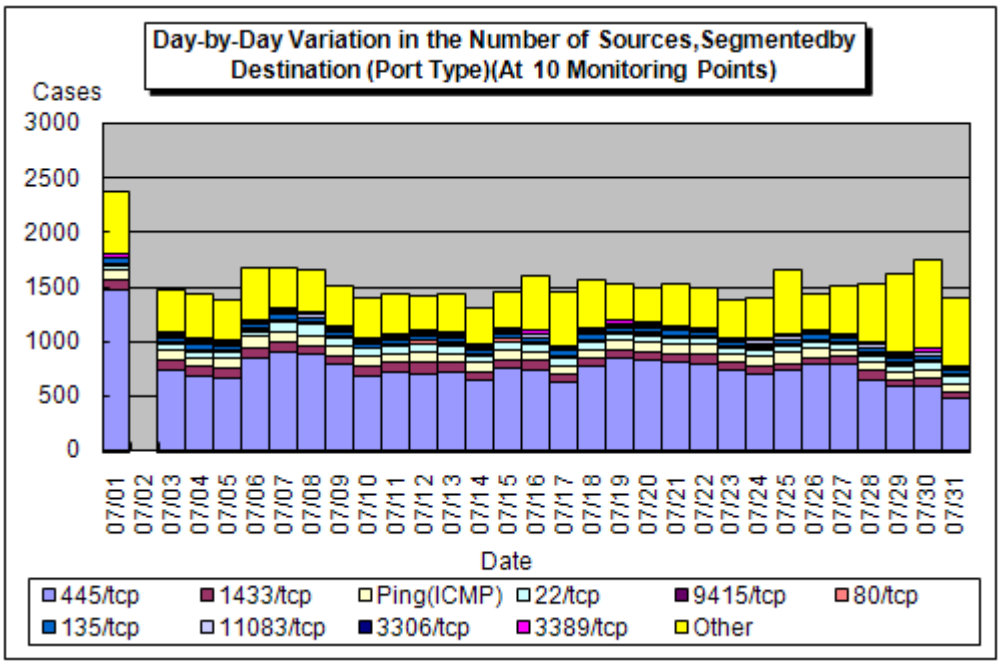

Figure2-2: Day-by-Day Variation in the Number of Sources, Segmented by Destination (Port Type) for July 2011

(2) Proportion of each Destination (Port Type)

Figure 2-3 shows the breakdown of the number of unwanted (one-sided) accesses by destination (port type) for July 2011. Figure 2-4 shows the breakdown of the number of sources by destination (port type) for July 2011. All the ratios shown in these figures are rounded to one decimal place, so they may not add up to 100 percent.

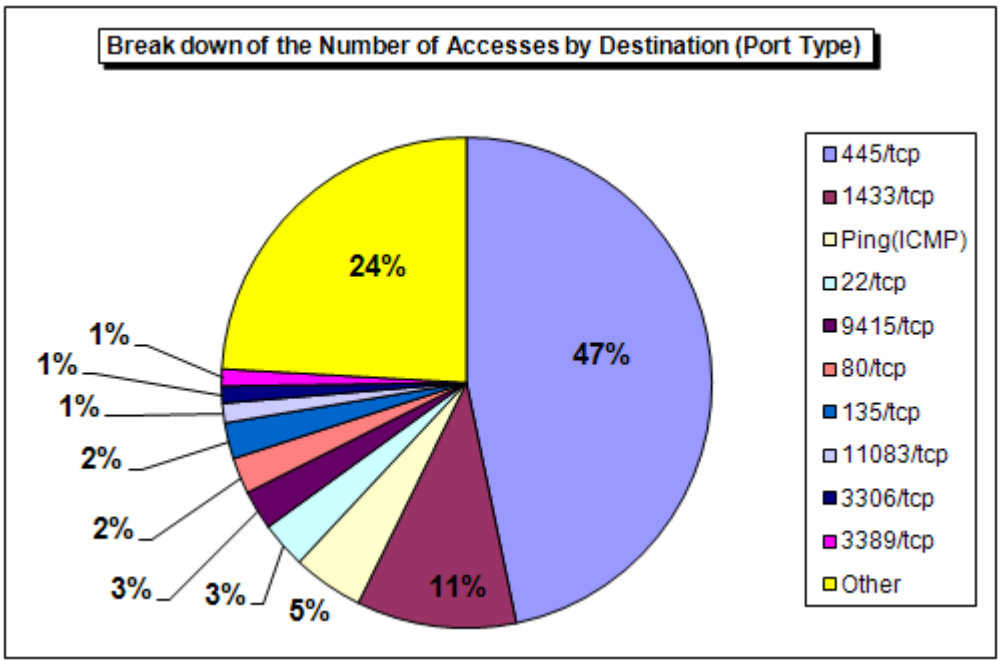

Figure2-3: Breakdown of the Number of Unwanted (One-Sided) Accesses by Destination (Port Type) for July 2011

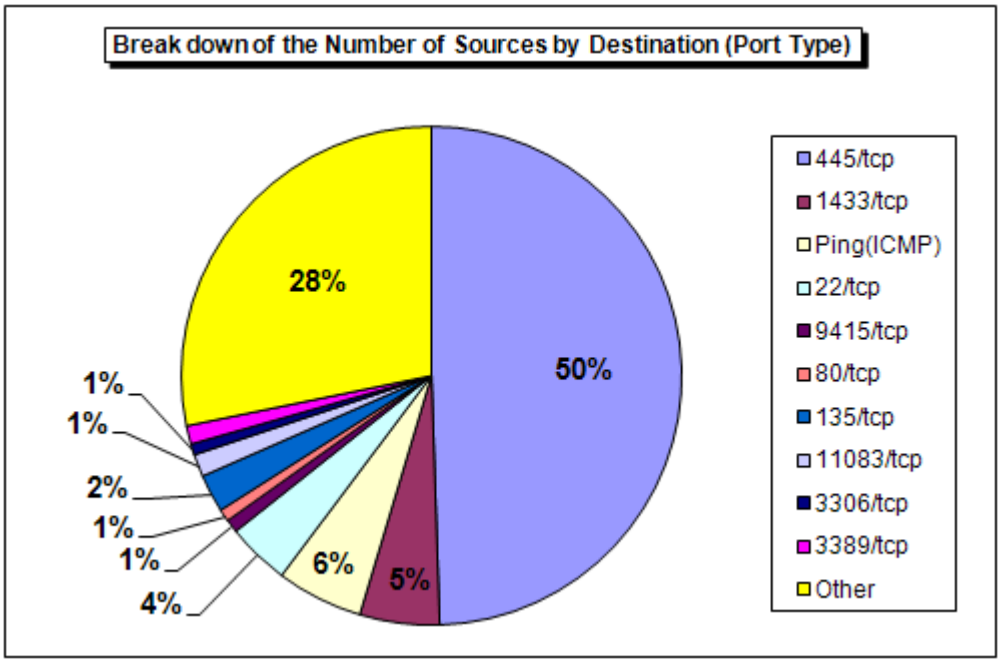

Figure2-4: Breakdown of the Number of Sources by Destination (Port Type) for July 2011

(3) Number of Accesses for each Country

Figure 2-5 shows the day-by-day variation in the number of accesses by country for July 2011. Figure 2-6 shows the breakdown of the number of access by country for July 2011. All the ratios shown in these figures are rounded to one decimal place, so they may not add up to 100 percent.

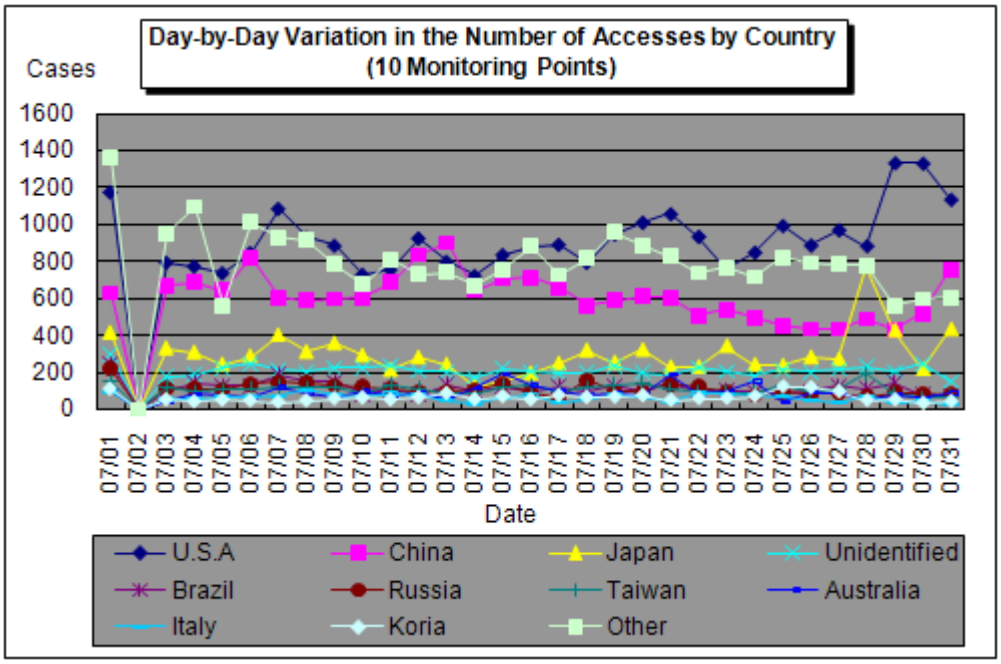

Figure2-5: Day-by-Day Variation in the Number of Accesses by Country for July 2011

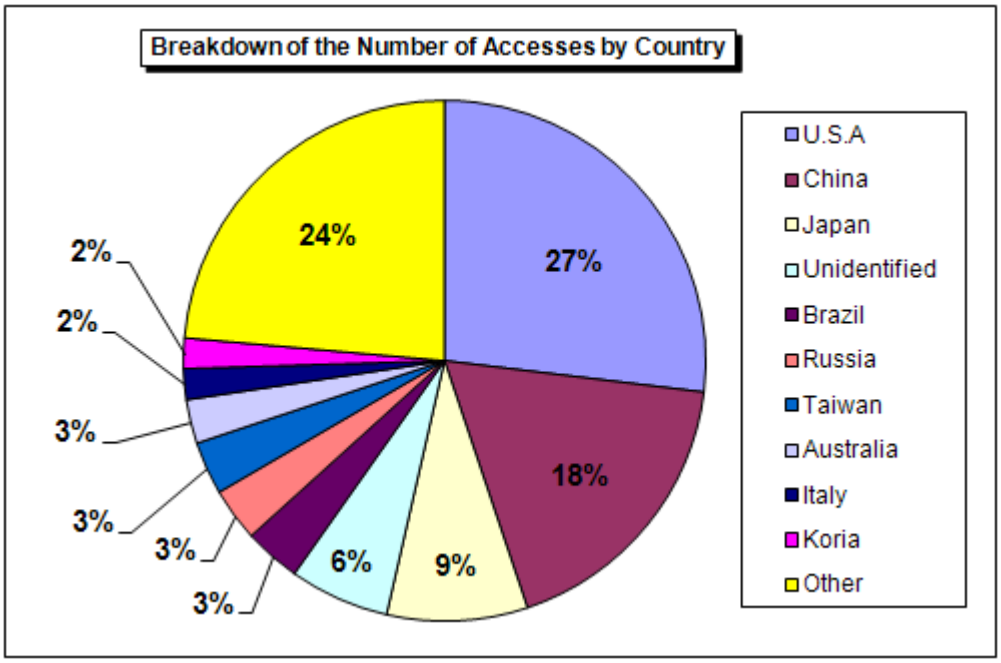

Figure2-6: Breakdown of the Number of Access by Country for July 2011

Figure 2-7 shows the day-by-day variation in the number of sources by country for July 2011. Figure 2-8 shows the breakdown of the number of sources by country for July 2011. All the ratios shown in these figures are rounded to one decimal place, so they may not add up to 100 percent.

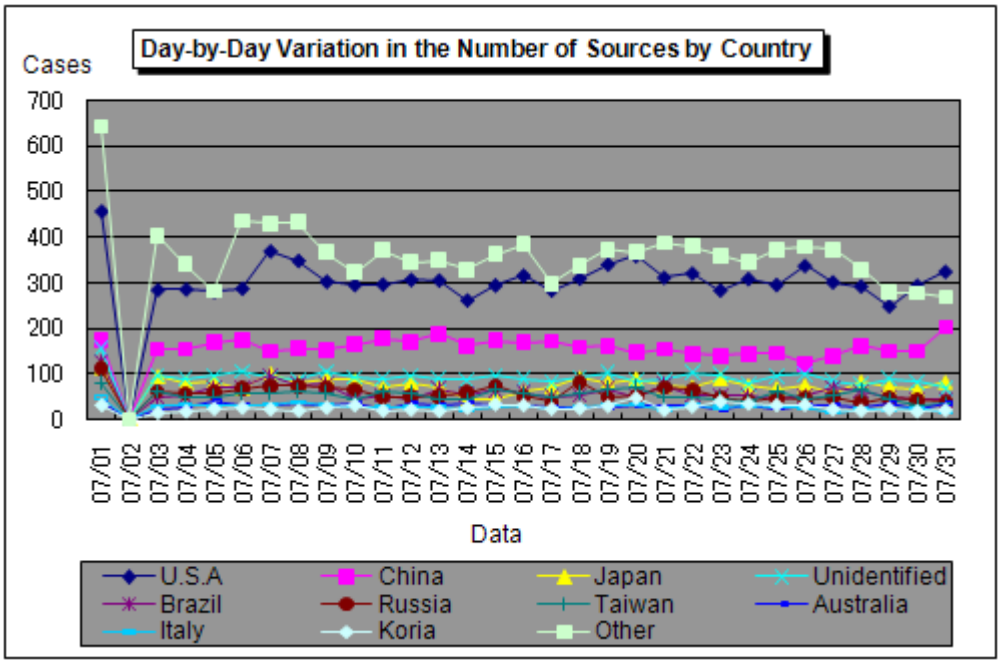

Figure2-7: Day-by-Day Variation in the Number of Sources by Country for July 2011

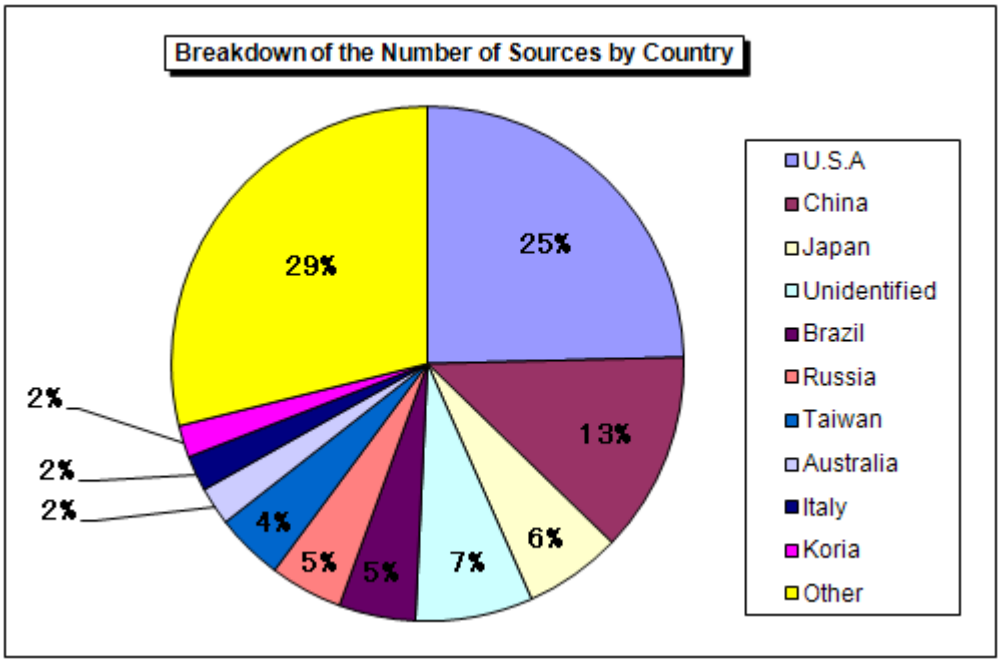

Figure2-8: Breakdown of the Number of Sources by Country for July 2011

3. Statistical Information

(1) Proportion of each Destination (Port Type)

Figure 3-1 shows the breakdown of the number of accesses by destination (port type) (from February 2011 to July 2011). Figure 3-2 shows the breakdown of the number of sources by destination (port type) (from February 2011 to July 2011).

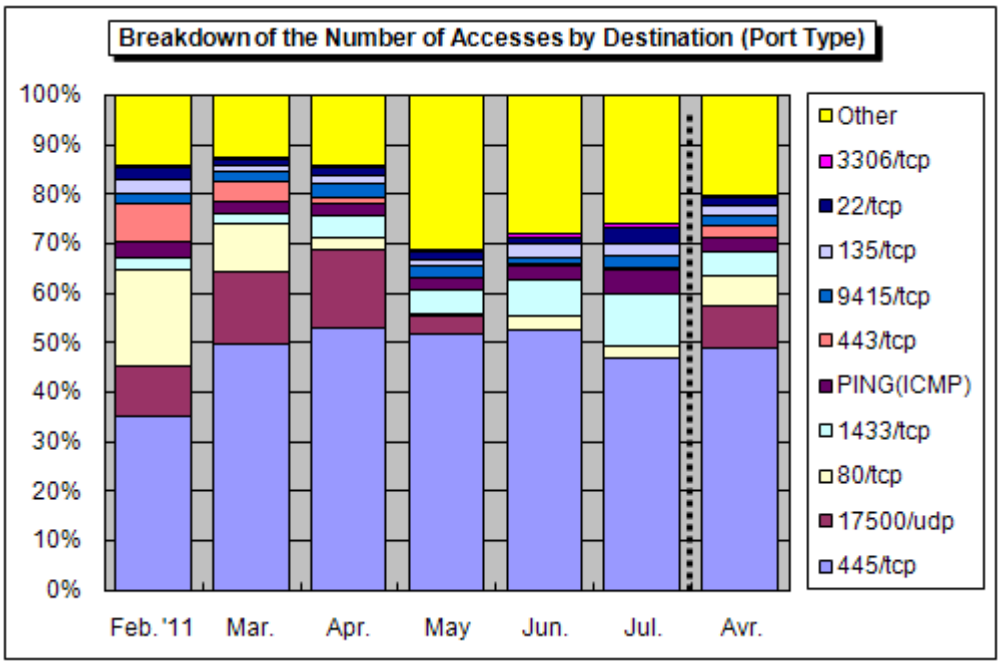

Figure3-1: Breakdown of the Number of Accesses by Destination (Port Type) (From February 2011 to July 2011)

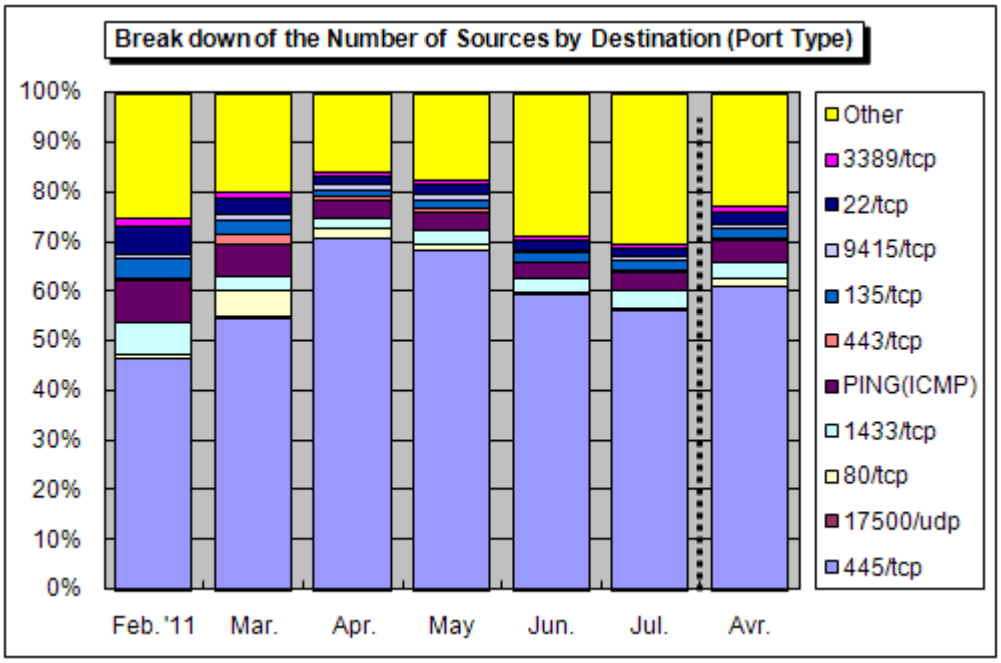

Figure3-2: Breakdown of the Number of Sources by Destination (Port Type) (From February 2011 to July 2011)

(2) Proportion by Country

Figure 3-3 shows the breakdown of the number of accesses by country (from February 2011 to July 2011). Figure 3-4 shows the breakdown of the number of sources by country (from February 2011 to July 2011).

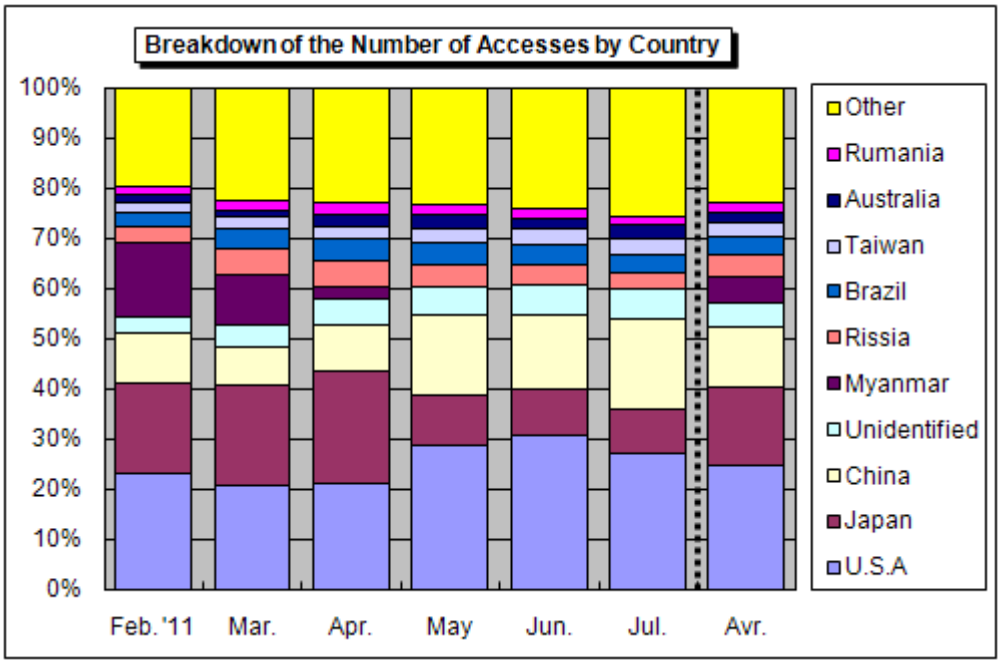

Figure3-3: Breakdown of the Number of Accesses by Country (From February 2011 to July 2011)

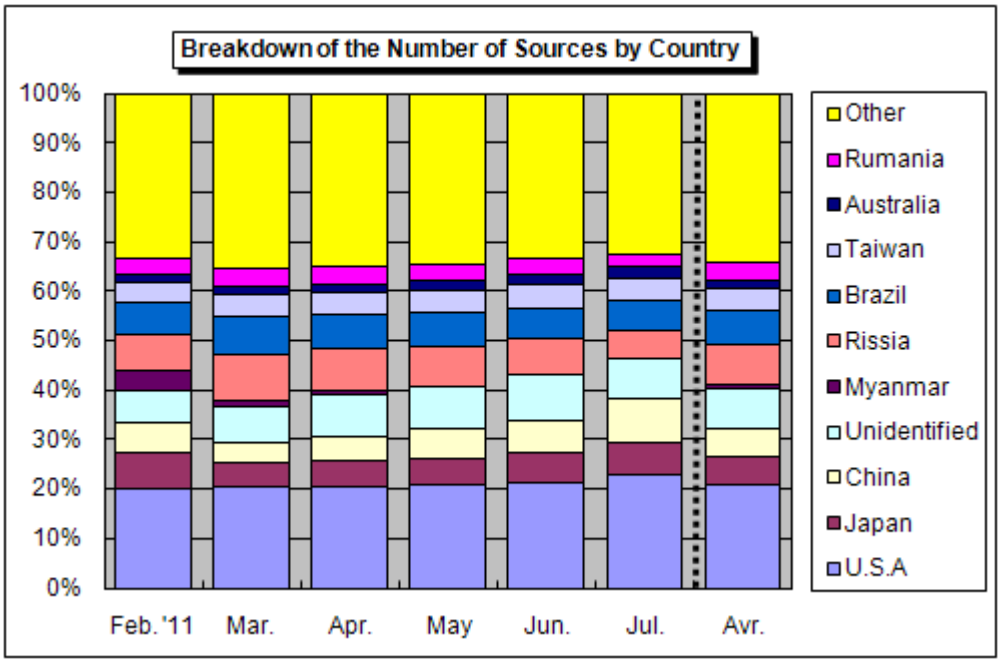

Figure3-4: Breakdown of the Number of Sources by Country (From February 2011 to July 2011)

4. Supplementary Explanations

The table below outlines the destinations (port types) frequently accessed in July 2011.

Port Type	Interpretations/Descriptions
445/tcp	Well known for unauthorized computer access through the exploitation of a vulnerable file (network) sharing mechanism or vulnerability specific to Windows 2000. (e.g., W32/Sasser) This port can be targeted by Worm exploiting the Windows vulnerability "MS08-067". (e.g., W32/Downad)
1433/tcp	This is the default port for Microsoft SQL Servers and it is highly likely that access to this port has been made for the purpose of searching for computers running SQL server or exploiting a vulnerability in SQL Servers.
Ping（ICMP）	Used to check if a specific computer is in operation (i.e., reachable) and known to have been exploited by W32/Welchia etc. to search for exploitable PCs for unauthorized access
22/tcp	Access to this port has been made by an attacker to break into a system by using password cracking through the exploitation of vulnerability in SSH - a protocol for communicating with a remote computer via the network.
9415/tcp	It is possible that, access to this port was made by an attacker to search for any PC running software program with the proxy feature that is posted on a Website in China, so he could use it to attack a Web server, etc.
80/tcp	This port is used by HTTP which is a protocol for Web access and it is highly likely that access to this port is made for the purpose of exploiting a vulnerability in an Web application or carrying out DoS attack.
135/tcp	This is the default port for the Microsoft Windows Remote Procedure Call (RPC) and well known for unauthorized computer accesses (W32/MSBlaster) through the exploitation of the RPC vulnerability (MS03-026).
11083/tcp	Access to this port was mainly made from multiple sources (IP address) in the U.S and China and was monitored at a single monitoring point for TALOT2. Purpose of this access remains unknown.
3306/tcp	This is the default port for MySQL Servers and it is highly likely that access to this port has been made for the purpose of searching for computers running MySQL server or exploiting a vulnerability in MySQL Server.
3389/tcp	This is the default port for Microsoft Windows-Based Terminal Server and it is possible that access to this port was made by an attacker to exploit this feature.

Inquiries to:
IT Security Center, Information-technology Promotion Agency, Japan (IPA/ISEC)
Kagaya/Ooura
Tel.: +81-3-5978-7591
Fax: +81-3-5978-7518
E-mail: isec-info@ipa.go.jp