

**Observation by Internet Fix-Point Monitoring System (TALOT2)
for May 2010**

1. To General Internet Users

According to the Internet Fixed-Point Monitoring System (TALOT2), **125,020** unwanted (one-sided) accesses were observed at ten monitoring points in May 2010 and the total number of sources* was **49,574**. This means on average, **403 accesses** form **160 sources** were observed at **one monitoring point per day**. (See Figure 1-1)

*Total number of sources: indicates how many accesses 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.

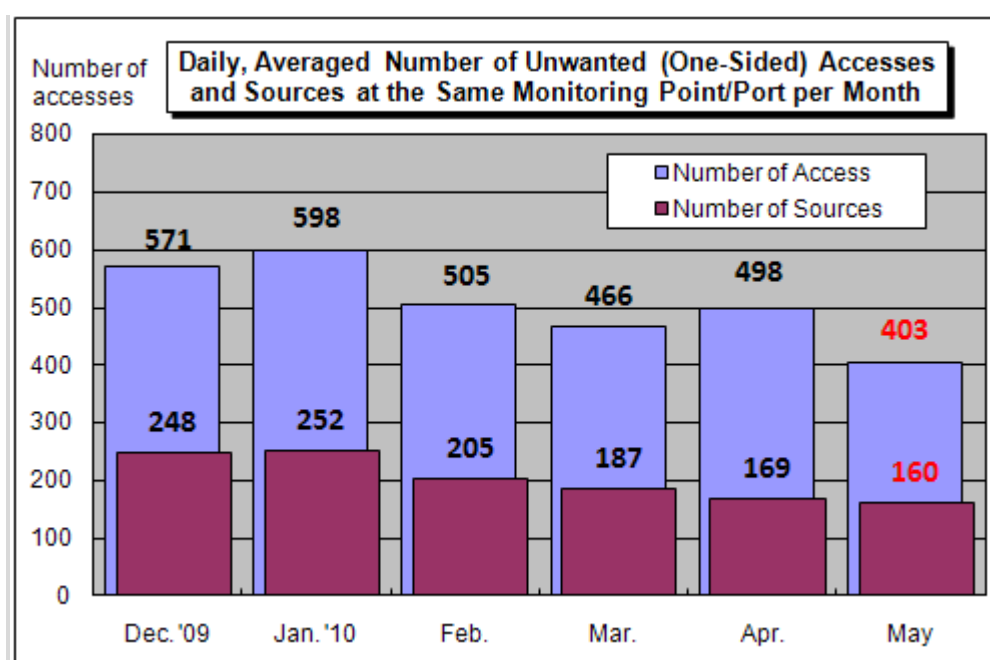


Figure1-1: Daily, Averaged Number of Unwanted (One-Sided) Accesses and Sources at the Same Monitoring Point/Port per Month

Figure 1-1 shows daily, averaged number of unwanted (one-sided) accesses and sources at the same monitoring point/port per month (from December 2009 to May 2010). As shown in this Figure, the number of unwanted (one-sided) accesses decreased in May compared to April.

Figure1-2 shows the May-over-April comparison results for the number of unwanted (one-sided) accesses, classified by destination (port type). As shown in this Figure, access to 9415/tcp and 21329/tcp, which wasn't ranked high in the past, has been ranked high in May. It has yet to be identified why these ports were accessed as they are not the ones used by a specific application.

As for 9415/tcp, access from multiple sources in overseas (mainly China) observed at multiple monitoring points of TALOT2 has been on the rise since March. (See Figure 1-3) Similar increasing trends have also been observed by other organizations undertaking fixed point observations, indicating that such access was made in widely-scattered areas, so we need to pay attention to observations status on an ongoing basis.

As for 21329/tcp, access from a single source in the U.S observed at a single monitoring point of TALOT2 have increased rapidly in May.

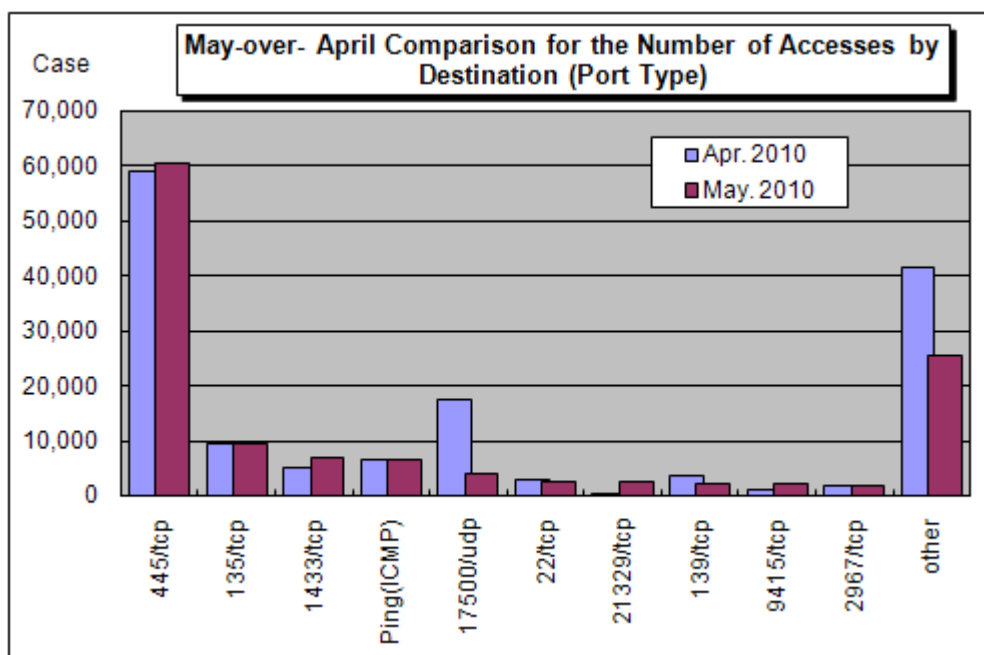


Figure 1-2: May-over-April Comparison for the Number of Accesses for each Destination (Port Type)

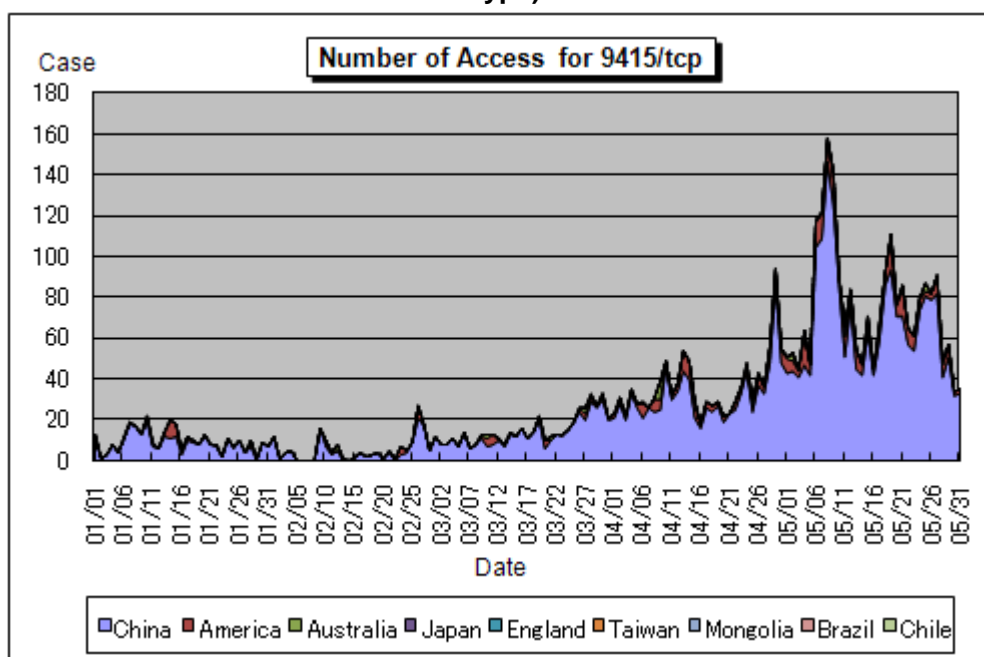


Figure 1-3: Number of Access for 9415/tcp

2. Unwanted(One-Sided) Access Observed in May 2010

(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 May 2010. Figure 2-2 shows the day-by-day variation in the number of sources.

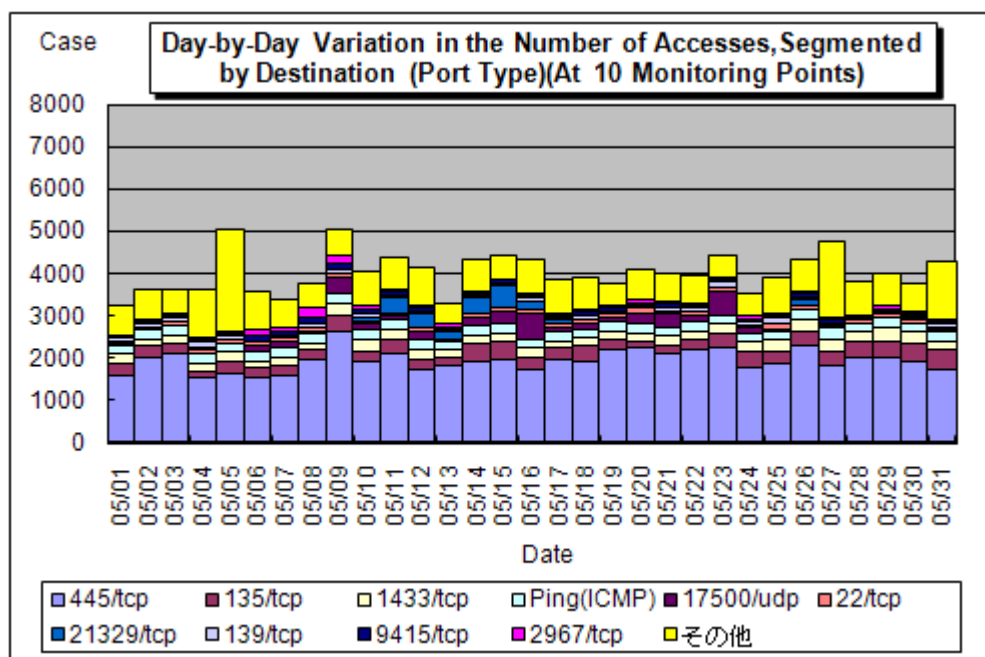


Figure2-1: Day-by-Day Variation in the Number of Accesses, Segmented by Destination (Port Type)(At 10 Monitoring Points)

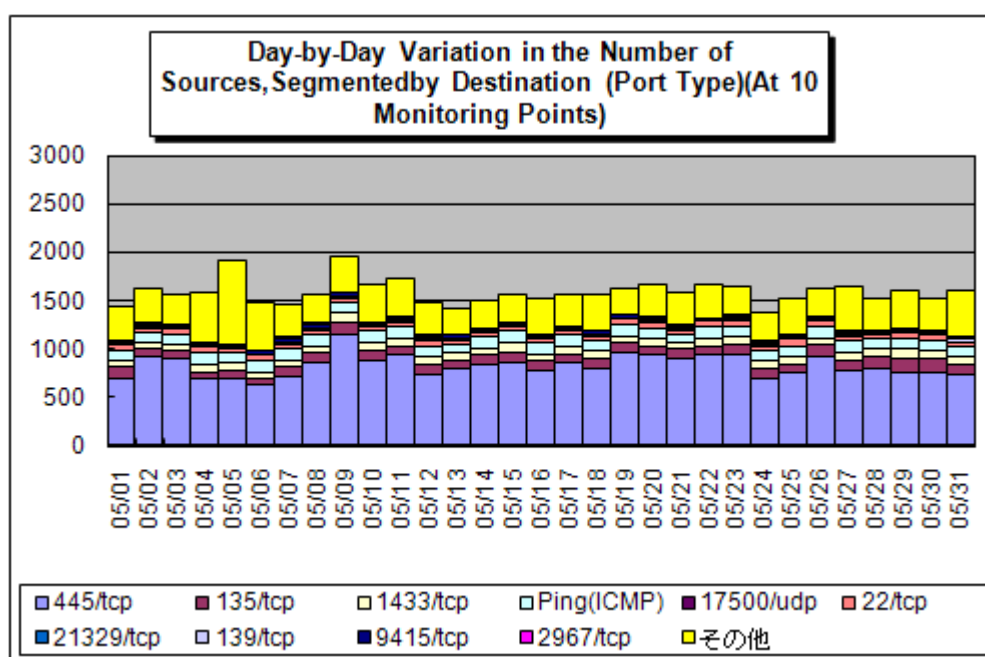


Figure2-2: Day-by-Day Variation in the Number of Sources, Segmented by Destination (Port Type), for May 2010

(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 May 2010. Figure 2-4 shows the breakdown of the number of sources by destination (port type) for May 2010. All the ratios shown in these figures are rounded to one decimal place, so they may not add up to 100 percent.

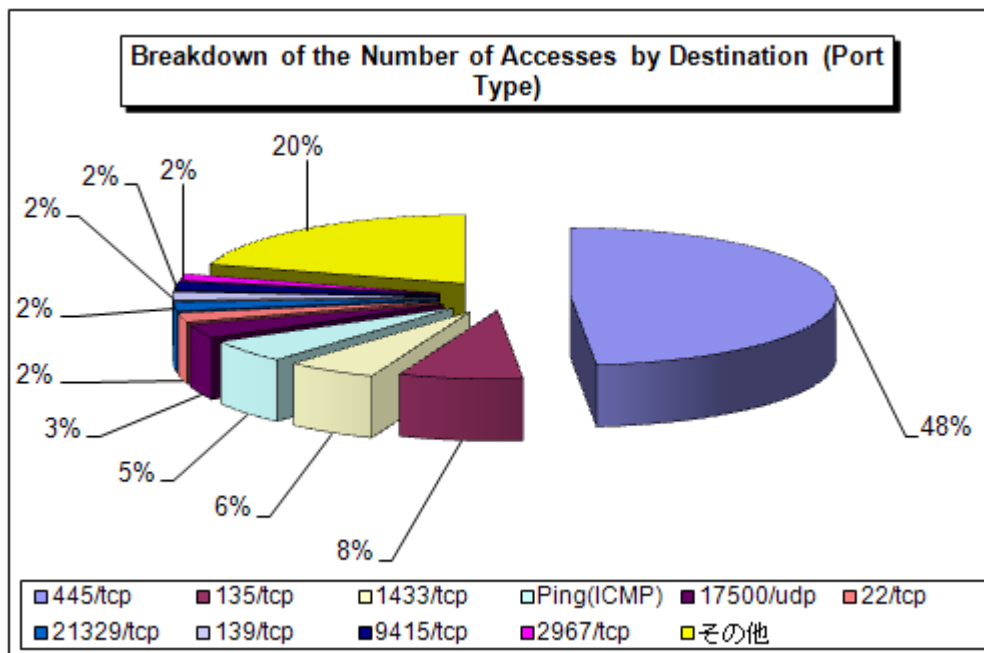


Figure2-3: Breakdown of the Number of Unwanted (One-Sided) Accesses by Destination (Port Type) for May 2010

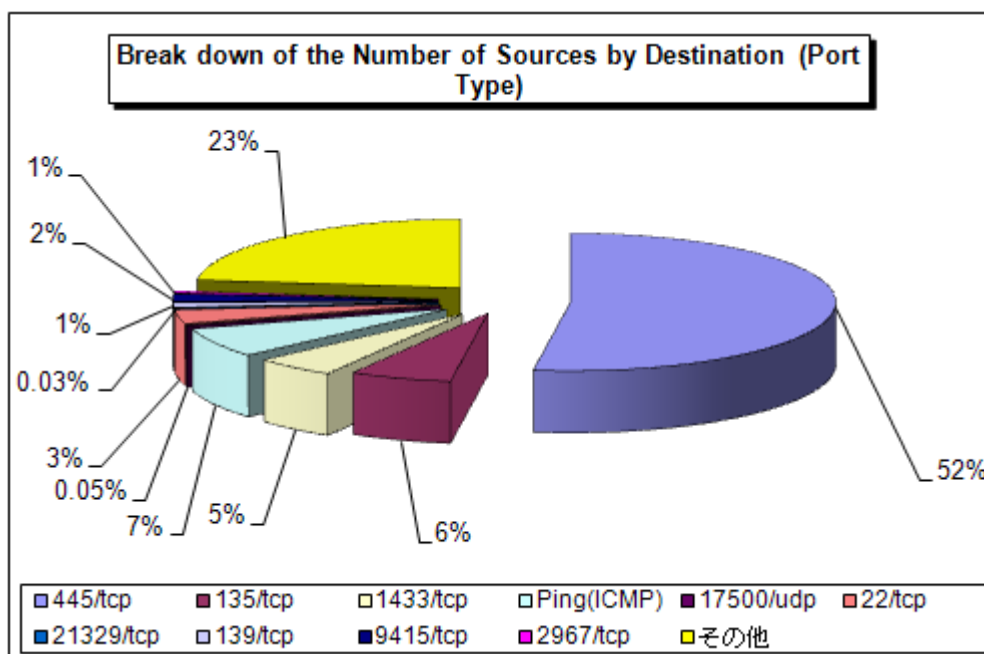


Figure2-4: Breakdown of the Number of Sources by Destination (Port Type) for May 2010

(3) Number of Accesses for each Country

Figure 2-5 shows the day-by-day variation in the number of accesses by country for May 2010. Figure 2-6 shows the breakdown of the number of access by country for May 2010. All the ratios shown in these figures are rounded to one decimal place, so they may not add up to 100 percent.

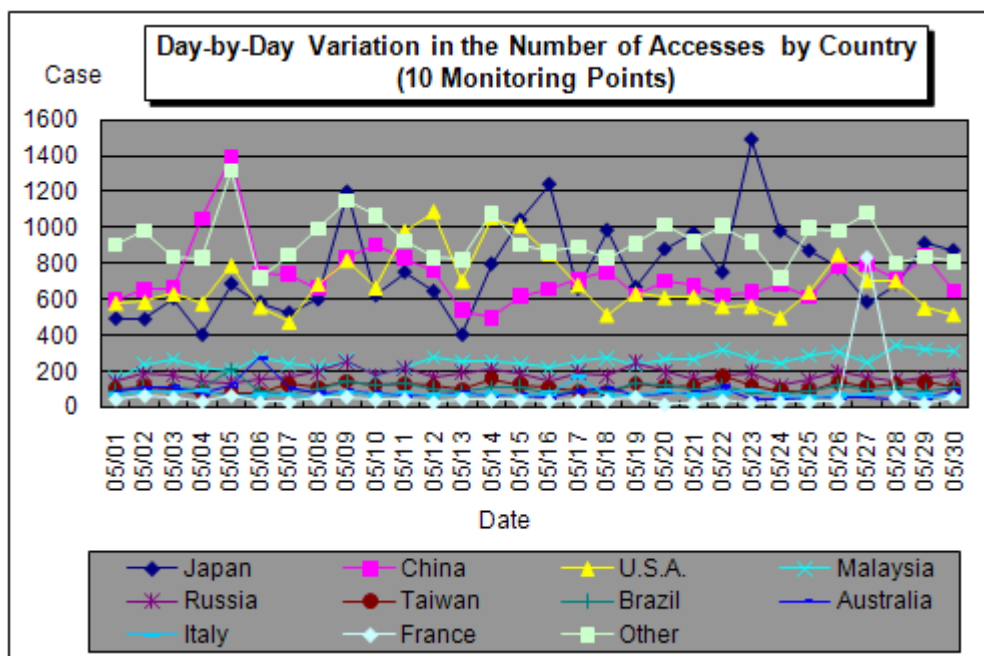


Figure2-5: Day-by-Day Variation in the Number of Accesses by Country for May 2010

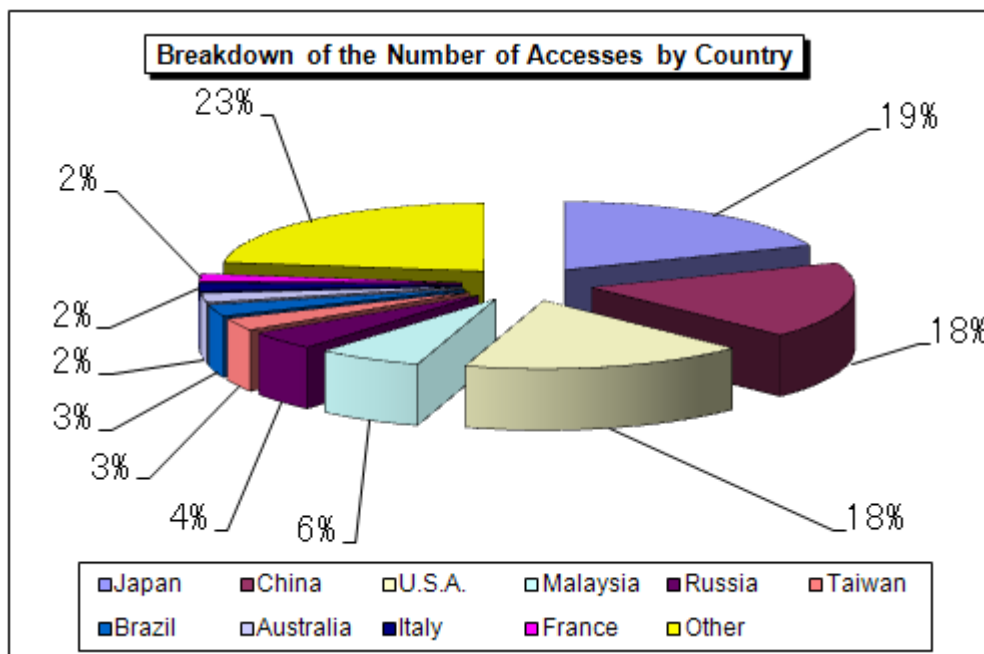


Figure2-6: Breakdown of the Number of Access by Country for May 2010

Figure 2-7 shows the day-by-day variation in the number of sources by country for May 2010. Figure 2-8 shows the breakdown of the number of sources by country for May 2010. All the ratios shown in these figures are rounded to one decimal place, so they may not add up to 100 percent.

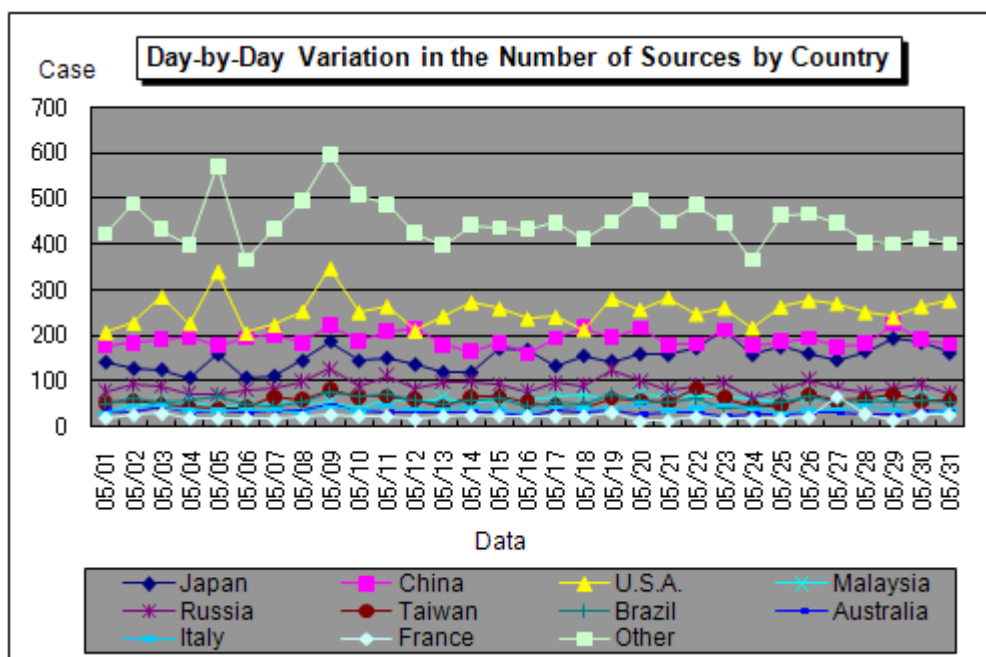


Figure2-7: Day-by-Day Variation in the Number of Sources by Country for May 2010

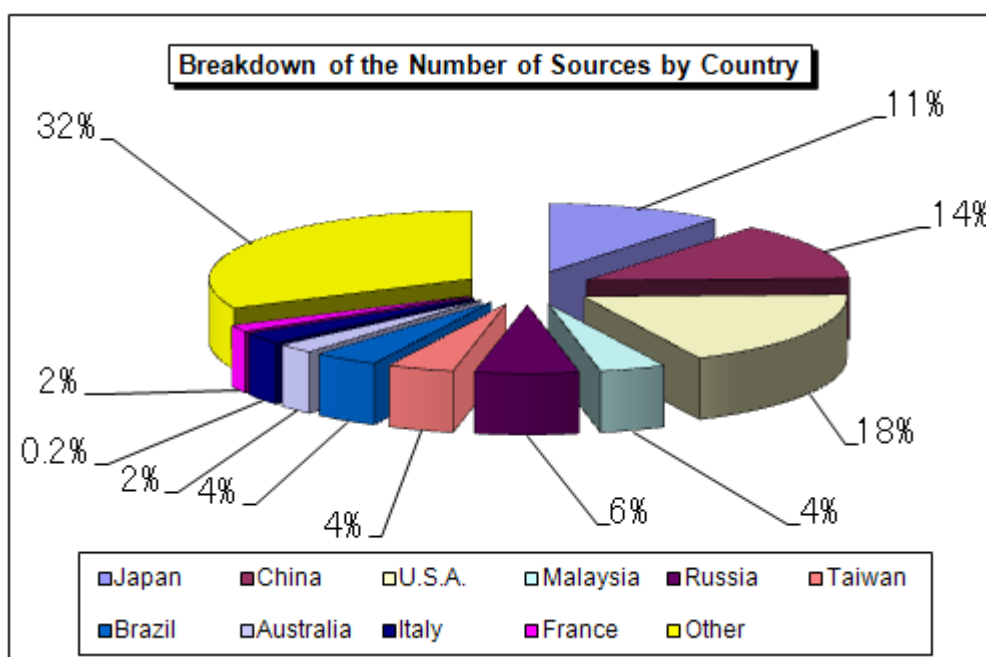


Figure2-8: Breakdown of the Number of Sources by Country for May 2010

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 December 2009 to May 2010). Figure 3-2 shows the breakdown of the number of sources by destination (port type) (from December 2009 to May 2010).

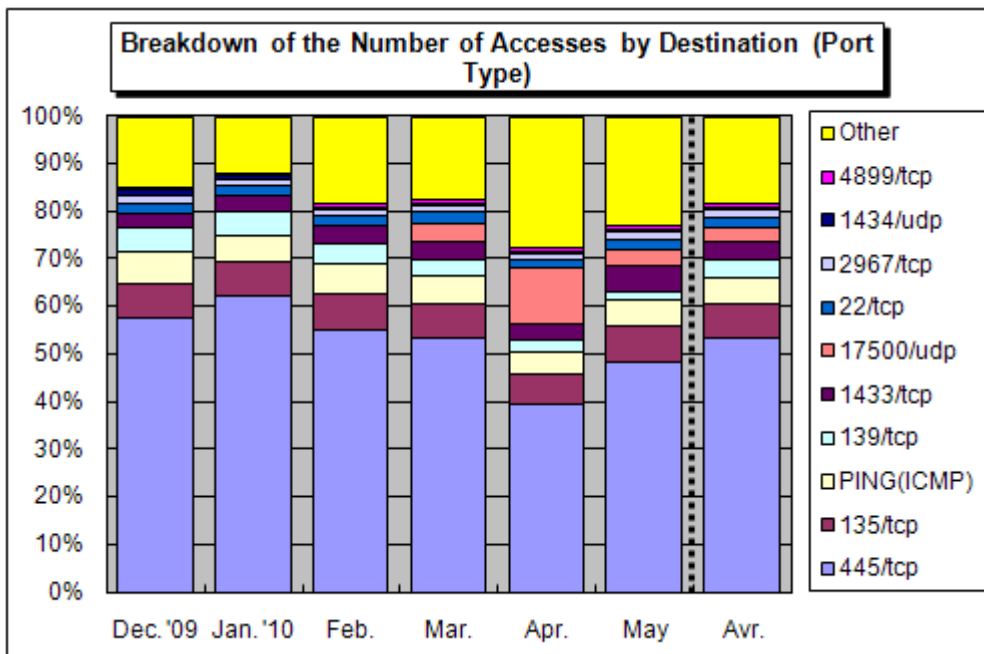


Figure3-1: Breakdown of the Number of Accesses by Destination (Port Type) (From December 2009 to May 2010)

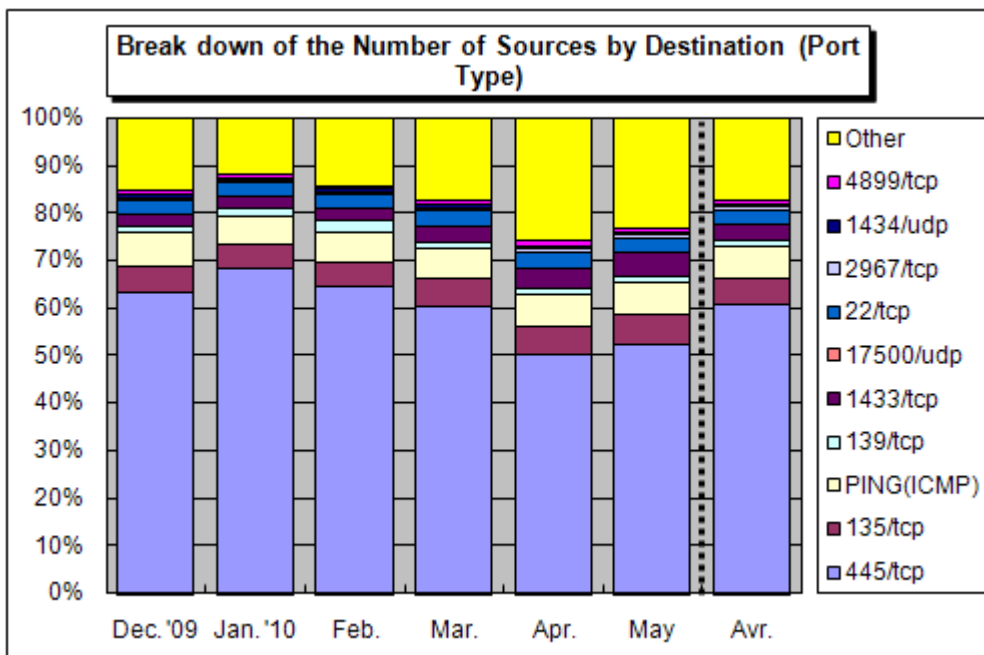


Figure3-2: Breakdown of the Number of Sources by Destination (Port Type) (From December 2009 to May 2010)

(2) Proportion by Country

Figure 3-3 shows the breakdown of the number of accesses by country (from December 2009 to May 2010). Figure 3-4 shows the breakdown of the number of sources by country (from December 2009 to May 2010).

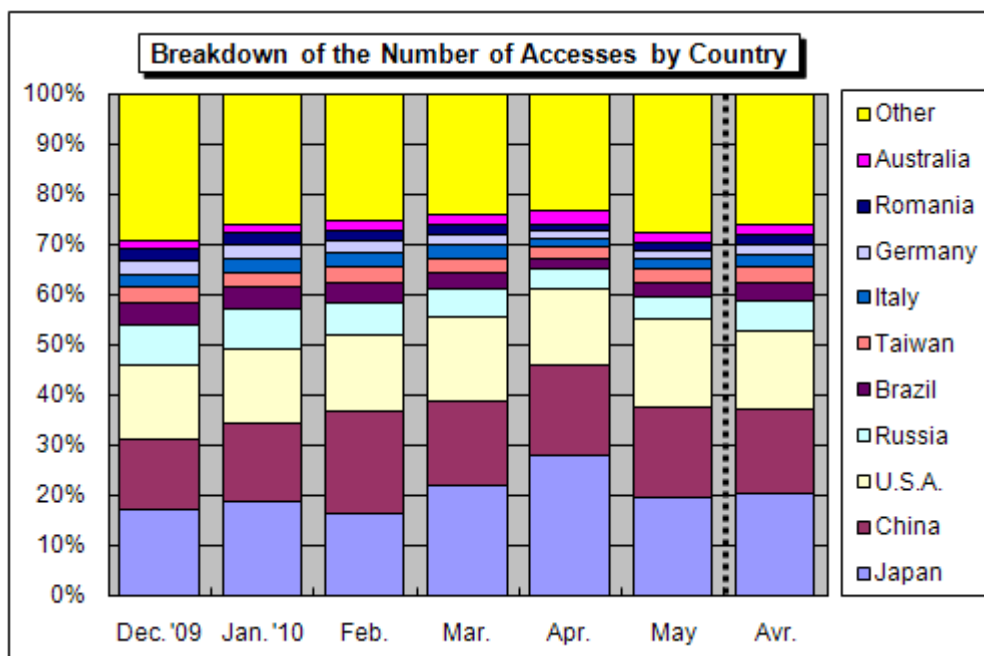


Figure3-3: Breakdown of the Number of Accesses by Country (From December 2009 to May 2010)

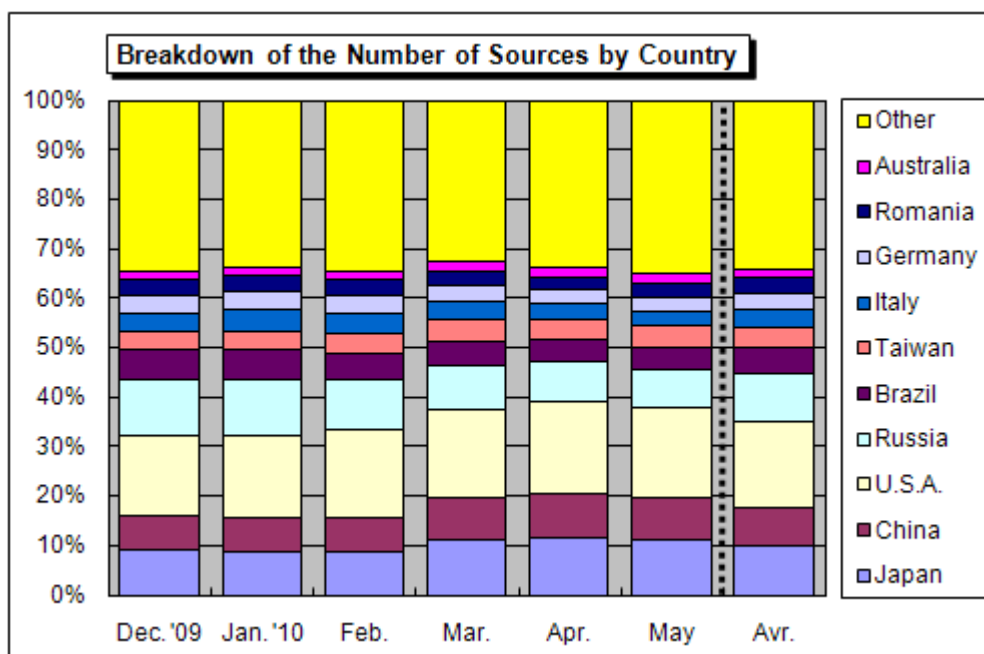


Figure3-4: Breakdown of the Number of Sources by Country (From December 2009 to May 2010)

4. Supplementary Explanations

The table below outlines the destinations (port types) frequently accessed in May 2010.

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)
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).
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 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
17500/udp	Access to this port has been observed at a single monitoring point since March 2010. Thought to be a broadcast being transmitted from a specific source.
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 - communication protocol for connecting to remote computers over a network
21329/tcp	In the middle of May, access to this port from a single source in the U.S was observed at a single monitoring point of TALOT2 and the purpose/objective of this access is still unknown.
139/tcp	Well known for unauthorized computer access through the exploitation of a vulnerable file (network) sharing mechanism and it is highly likely that access to this port is generally made to exploit vulnerability in Windows.
9415/tcp	Access to this port has been on the rise since around March. Access was made from multiple sources in overseas (mainly China) and observed at multiple monitoring points of TALOT2. The purpose/objective of this access is still unknown.
2967/tcp	It is highly likely that access to this port has been made for the purpose of exploiting vulnerability in Symantec products such as Symantec Client Security and Symantec Antivirus, etc.

Inquiries to:

IT Security Center, Information-technology Promotion Agency,
 Japan (IPA/ISEC)
 Ooura/Hanamura/Kagaya
 Tel.: +81-3-5978-7527
 Fax: +81-3-5978-7518
 E-mail: isec-info@ipa.go.jp