

Computer Virus/Unauthorized Computer Access
Incident Report - March 2009

This is the summary of computer virus/unauthorized computer access incident report for March 2009 compiled by IPA.

I. Reminder for the Month

“Do you know about “Security Alert Screen”?”
- There are some useful tips to prevent damages from malicious intents -

The consultation number relevant to “One-click billing fraud” rushed to IPA was temporarily decreased with the 651 cases which peaked in September 2008; however it was again drastically increasing for the last 4 months (See the Chart 1-1). In March, the cumulative consultation number for the “One-click billing fraud” was eventually exceeded 10,000 cases!

The one of the major causes is that several sites that use newer fraudulent method were appeared. With the newer method, computer configuration is altered so that it will be difficult to perfectly restore it to the original state.

Such site using newer method may be increased; however, the preventive measures against them are fundamentally the same. Accordingly, be sure to check the “Security Alert” screen along with the message displayed and be cautious to prevent from becoming a casualty.

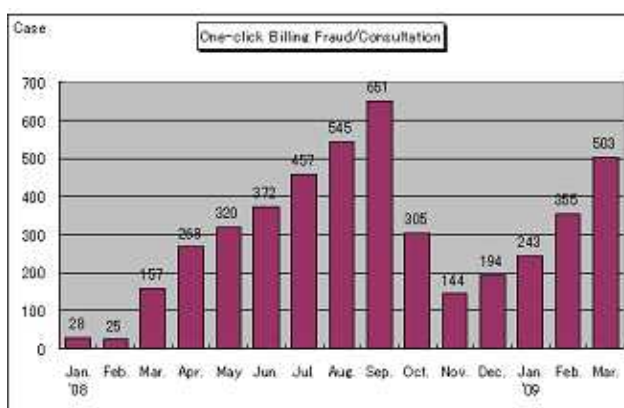


Chart 1-1: One-click Billing Fraud/Consultation

(1) What is “One-click Billing Fraud”?

“One-click Billing Fraud” is the illegally method to bill a user who clicks/forwards images over and over to browse animated movies in an adult site. Such method often exploits to induce users from (sound) animation and game sites other than adult sites: there rushes number of consultations to IPA regardless of users’ age and/or their gender.

(a) Traditional Method

Upon clicking the button for “Free” or “Sample” in the illegal site relevant to billing fraud, a malicious program (i.e. in.exe format, etc.) such as virus, etc. which display billing screen will be downloaded and installed. In the event, upon starting up your computer, the malicious program will automatically be executed and thus the billing screen is appeared every time when starting up your computer. (Though the computer is not connected to the Internet, the billing screen will be appeared.)

To address against such problem, you are to delete the program being installed. In most of cases, your anti-virus software will work out even infected by virus.

(b) Newer Method

The method newly emerged in February can alter computer configuration without installing malicious program (i.e., in .exe format, etc.) which differed from traditional ones: the malicious program will display the billing screen by automatically connecting to the adult site on the Internet exploiting a web browser when starting up your computer.



Chart 1-2: Inerasable Screen with Newer Method

The billing screen appeared on your computer with the newer method is unfriendly as you cannot close the screen with an “x” or move the screen to the end of the screen: you cannot erase the billing screen (See the Chart 1-2) as well. In that case, your anti-virus software cannot support such symptoms since your computer is not infected by virus.

To address this, “System Configuration Utility”^{*1} will be used to delete the command, i.e., the start up Item being added by the malicious program which automatically connects to an adult site on the Internet. In doing so, your computer will not automatically connect you to an adult site. To completely restore your computer’s configuration information, it is necessary to edit system configuration data (i.e. registry); your requisite programs may not work if you inadequately edit the data, so please be careful.

As mentioned above, once damaged, it must be a challenge to restore back your computer to the original state as it needs special engineering knowledge.

*1: The software which diagnoses and/or restores the problems in system configuration for Windows. By modifying the system configuration with the utility, the malicious program which automatically starts up upon Windows starting up can be cancelled. However, this utility is not available for Windows 2000.

(2) Measures

(a) Preventive Measures

The fundamental preventive measures is to carefully read the information appeared in the “File Downloads-Security Alert”, the one of Windows functions and do not easily click the “Execute” button (See the Chart 1-3). The “Alert” screen is not for replaying images or movies. The “Alert” screen is alerting you that some potentially malicious programs are being downloaded to your computer. If the alerting screen is appeared when you are browsing homepages, be sure to click “cancel” button so that the malicious programs will not be downloaded to your computer.

Even you can determine that the program is not malicious, be sure to save/download the program first and check it with your anti-virus software before open (i.e. execute) it.

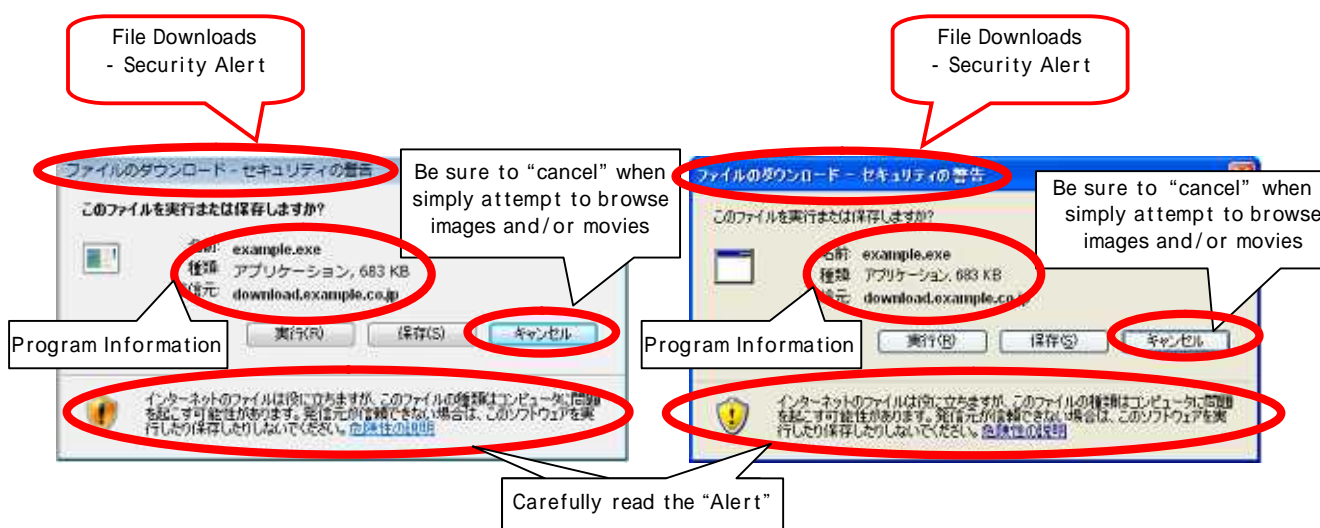


Chart 1-3: 2 Examples of “Security Alert” in the Internet Explorer

Of the websites in where some damage was reported, there confirmed that their methodology is further sophisticated as they prepare illustrated descriptions to have users easily click the “execute” button in the “Security Alert” screen with sweet talk (See the Chart 1-4). Be sure to read the information carefully and not to totally believe the descriptions on the adult site: if you feel suspicious, be sure not to go further.

This is not directly related to the instance above, most of the consultations rushed to IPA include that “the user did not read the information carefully though there clearly stated that the user will be charged at the adult site”, “eventually displayed billing screen as the user carelessly clicked to go forward as he believed he would not be “charged” .” Those users could have been prevented before something happened if they read the information on that adult site carefully (See the Chart 1-5).



Chart 1-4: Illustrated Description to Have Users Easily Click “Execute” Button



Chart 1-5: Charges at an Adult Site

(b) Post-Measures

Windows XP and Windows Vista furnish system restoration function. The problem can be resolved by restoring the system to the original state before such billing screen is appeared.

<Reference>

“Using System Restore” (Microsoft)

<http://www.microsoft.com/windowsxp/using/setup/support/sysrestore.msp>

In case system restoration does not normally completed, you may edit system configuration data (registry): however, your computer may not be started up if the data wrongly be edited. If you are not familiar with (i.e. you are not confident), you’d better to leave them as they are.

In addition, if you do not know how to address the symptoms, please consult with IPA. As we provide general users a consultation session by telephone, be sure to call us with your computer be operable.

Computer Virus Dial 110 (Emergency Call)

Tel.: 03-5978-7509 (24-hour automatic response, in person consultation is available for the hours of 10:00 12:00 and 13:30 17:00 from Mon. to Fri.)

<Reference>

“Topics – Reminder relevant to One-click Billing Fraud” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/topics/alert20080909.html>

II. Reporting Status of Computer Virus - further details, please refer to the Attachment 1 -

The detection number*¹ of virus in March was **about 119T** and was decreased 7.7% from about 128T in February. In addition, the reported number*² in March was **1,674** and was increased 14.4% from **1,463** in February.

*¹ Detection number: Reported virus counts (cumulative) found by a filer.

*² Reported number: Aggregated virus counts. Viruses of same type and their variants reported on the same day are counted as one case number regardless how many viruses or the actual number of viruses is found by the same filer on the same day. In March, the reported number was 1,674 and the aggregated virus count was about 1119T. *(From the May '08 report, we use "T (thousand)" instead of using "M (Million)" to specifically present the detection number of virus.)*

The worst detection number was for **W32/Netsky** with **about 105T**, **W32/Mytob** with **about 5T** and **W32/Mydoom** with **about 3T** followed.

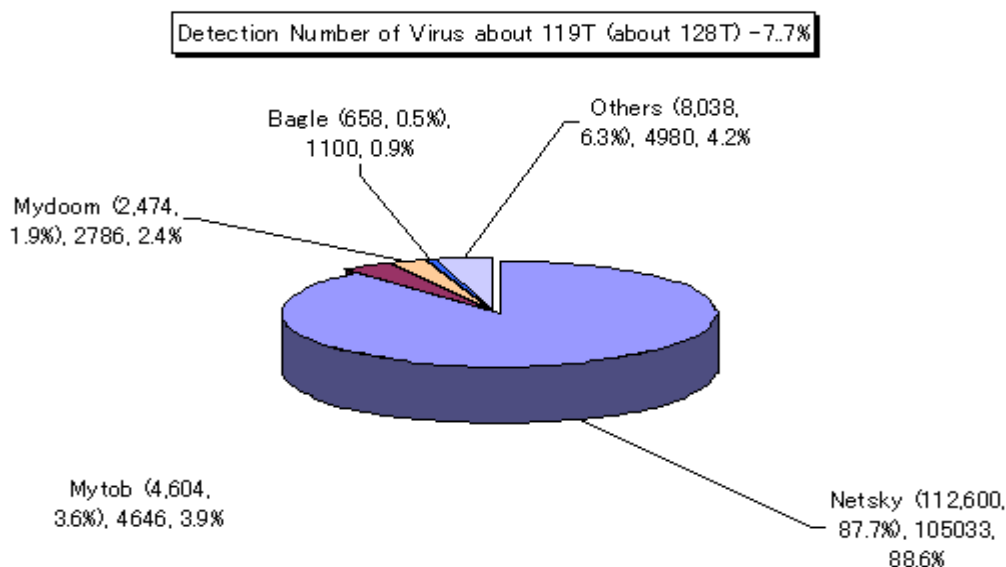


Chart 2-1: Detection Number of Virus (Numbers in parenthesis present the figures in previous month)

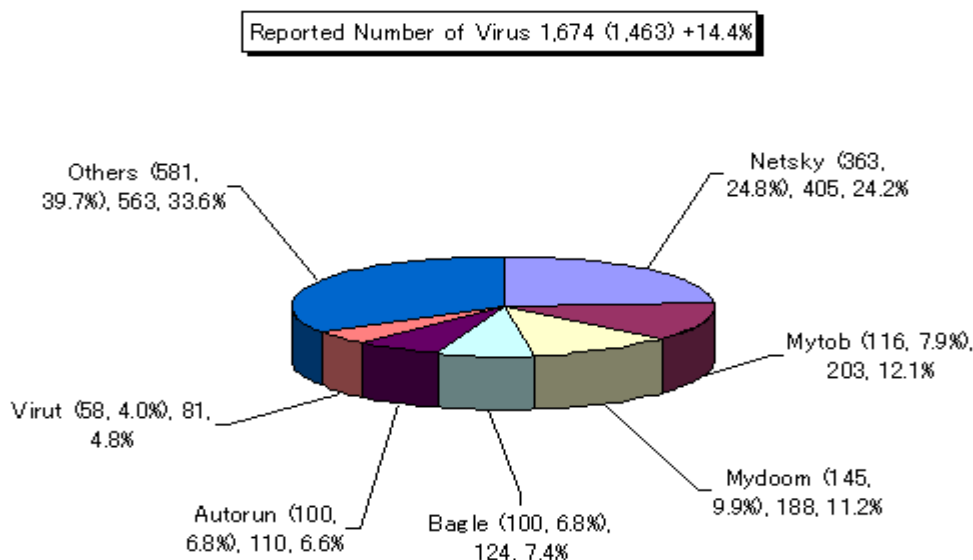


Chart 2-2: Reported Number of Virus (Numbers in parenthesis present the figures in previous month)

III. Reporting Status of Unauthorized Computer Access (includes Consultations) -

Please refer to the Attachment 2 for further details -

Chart 3-1: Report for unauthorized computer access and status of consultation

	Oct.	Nov.	Dec.	Jan. '09	Feb.	Mar.
Total for Reported (a)	17	18	10	10	9	20
Damaged (b)	12	12	7	7	6	13
Not Damaged (c)	5	6	3	3	3	7
Total for Consultation (d)	58	39	38	29	35	40
Damaged (e)	22	19	19	13	14	11
Not Damaged (f)	36	20	19	16	21	29
Grand Total (a + d)	75	57	48	39	44	60
Damaged (b + e)	34	31	26	20	20	24
Not Damaged (c + f)	41	26	22	19	24	36

(1) Reporting Status for Unauthorized Computer Access

Reported number in March was 20: Of 13 was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was 40 (of 3 was also counted as reported number): Of 11 was the number actually damaged.

(3) Status of Damage

The damage report included: by **intrusion** with **4** and by **embedding of malicious codes** with **9**.

The damage caused by “intrusion” included: some commands were executed on the server with 1, the server was exploited as a steppingstone to attack to the other site with 2 and the contents data in the web server was deleted with 1: those servers damaged were conducted by SQL injection attack respectively. The causes of intrusion were: exploited the vulnerability in that server with 1, seemed to be conducted by password cracking attack to the port used by SSH with 1, and by password cracking attack, but the others may have been targeted with 1 (as for the rest 1, the cause was not realized).

***SQL (Structured Query Language):**

The query language used to operate/define data in the relational database management system (RDBMS).

***SQL Injection:**

One of attacking methods exploiting vulnerability (ies) in the program which accesses to a database: this attack fraudulently browses and/or alters data within that database with the methods other than legitimate.

***SSH (Secure SHell):**

One of the protocols communicates with the computer remotely via a network.

***Password Cracking:**

The activity analyzes/parses the other individual's password. Brute Force attack (Exhaustive Search attack) and Dictionary attack are well known. There existed the program exclusively for password cracking.

(4) Damage Instance

[Intrusion]

(i) Seemed to be intruded by SQL injection attack...

Instance	<ul style="list-style-type: none"> - When checking logs with “iLogScanner”, the one of SQL injection detection tools provided by IPA; then several thousands of probes that showed successful attack are identified. It seems that the attack may have been conducted more than 6 months. - However, our management is seemed to be reluctant to disclose the instance so that we cannot pursuit following studies. - As the tentative measures, we stop publicizing the contents using database and start to review the web applications.
----------	---

(ii) Intruded and homepage related data was deleted...

Instance	<ul style="list-style-type: none"> - Study is conducted as the web pages being publicized by my business are getting unbrowsable; then it is realized that the directory for the homepage on the server was deleted. - Subsequently check the logs, some access attempts from the other IP addresses other than these being controlled by my business (i.e. from overseas) are identified. - The server is in modification/implementation processes for system configuration and for IDS* respectively to strengthen security.
----------	---

***IDS (Intrusion Detection System):**

The system detects/ notifies intrusion and invasion to systems.

IV. Accepting Status of Consultation

The gross number of consultation in March was 1,406. Of the consultation relevant to “One-click Billing Fraud” was 503 (February: 355), consultation relevant to “Hard selling of falsified anti-virus software” was 3 (February: 17), consultation relevant to “Winny” with 6 (February: 7), were realized. (The consultation relevant to “the suspicious mail sent to specific organization to collect specific information/data” was 1 (February: 5).

Chart 4-1: All the Consultation Number Accepted by IPA over the Past 6 Months

	Oct.	Nov.	Dec.	Jan. '09	Feb.	Mar.
Total	1171	713	839	960	1,051	1,406
Automatic Response System	677	363	458	529	521	758
Telephone	441	288	331	390	472	597
e-mail	47	62	49	39	57	49
Fax, Others	6	0	1	2	1	2

*IPA consults/advises about computer viruses, unauthorized computer accesses, problems relevant to Winny as well as the other information concerning overall security issues.

Mail: virus@ipa.go.jp for virus issues, crack@ipa.go.jp for crack issues, winny119@ipa.go.jp for emergent consultation relevant to Winny, fushin110@ipa.go.jp for suspicious mail handling and isec-info@ipa.go.jp for other security relevant issues.

Tel.: +81-3-5978-7509 (24-hour automatic response; in person consultation by an IPA Security Center personnel is available from Mon. - Fri., 10:00 - 12:00, 13:30 - 17:00.)

Fax: +81-3-5978-7518 (24-hour automatic response)

*"Automatic Response System": Numbers responded by automatic response

*"Telephone": Numbers responded by the Security Center personnel

*The Total case number includes the number in Consultation (d) column of the Chart in the “III. Reported Status for Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

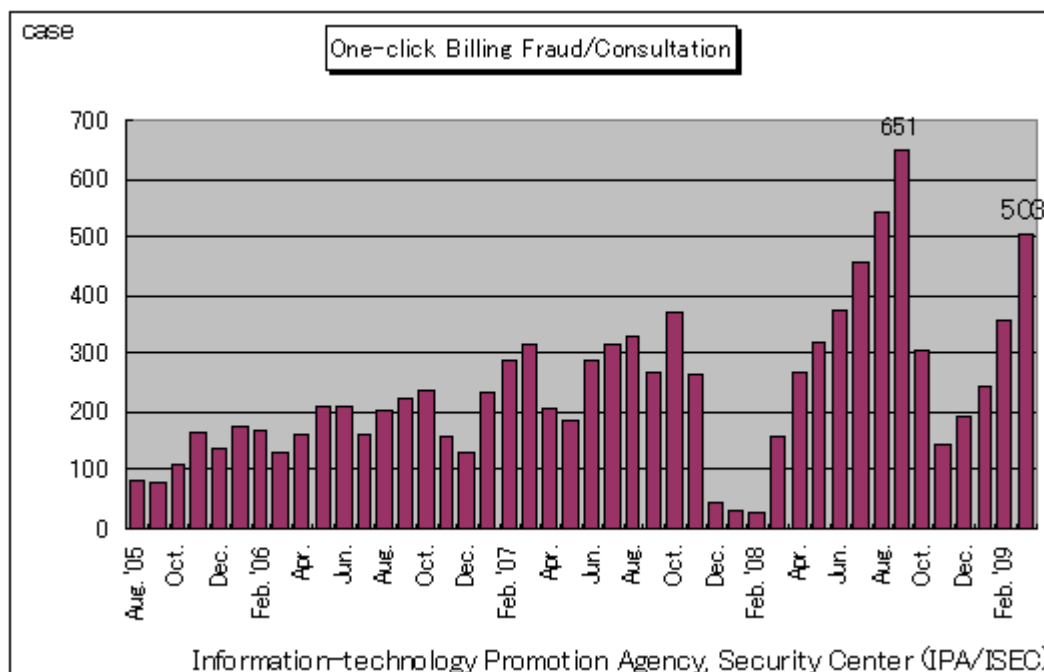


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) Data created by myself is deviated on the Internet...?

Consultation	When I search some information with Google engine, the list of name file, the diary file, etc. seem to be created by myself were hit. My computer may have been infected by virus and data was deviated on the Internet?
Response	The data (file) stored in your computer may be appeared as the search result. It seemed that the application so called "Google Desktop" may be installed in your computer. With this application, every data (file) stored in general users' computers can also be the subject for the search engine. The application may be pre-installed in some of the current computer model. You can check the program inventory being stored in your computer from the control panel.

(ii) Are there any anti-virus software available for Windows 98 and Me...?

Consultation	I am not a frequent computer user: I only send/receive mails and sometimes browse homepages so that I am still using Windows 98. Since I am worrying about virus so that I wish to install anti-virus software, but the software supportable for Windows 98 is not available in a store. What should I do?
Response	<p>We do not recommend the further use of Windows 98 and Me as their security problems (i.e. vulnerabilities) will not be resolved: since their supporting period is already concluded so that none of modification programs will be provided if vulnerabilities are detected in the future. Depending on the types of vulnerabilities, you may be infected by virus when you simply connect to the Internet. In addition, you may be infected when you simply browse some malicious sites. The principle of security measures is to resolve these vulnerabilities. In another words, any security measures will not efficiently work out if vulnerabilities are not resolved. We often hear that "there's no problem as my computer is not connected to the Internet." from many users, but the concept is not always true. Since nowadays, we have number of opportunities to exchange data via an USB memory and number of virus which infects via an USB memory is going around.</p> <p><Reference></p> <p>IPA - The Seven Anti-virus Requirements for Computer Users (in Japanese) http://www.ipa.go.jp/security/antivirus/7kajonew.html</p>

V. Accessing Status Captured by the Internet Monitoring (TALOT2) in March

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in March was **136,437** for the 10 monitoring points and the gross number of source* was **44,646**. That is, the number of access was **444** from **144** source addresses/monitoring point/day.

*Gross number of source: the gross number of the source accessed the TALOT2. In addition, the source will be counted as 1 if accessed from identical source in the same day to the same point/port.

Since each monitoring environment for the TALOT2 is nearly equal to the general connection environment used by the Internet; it can be considered that the same amount of unwanted (one-sided) access can be monitored for the general Internet users' connection environment.

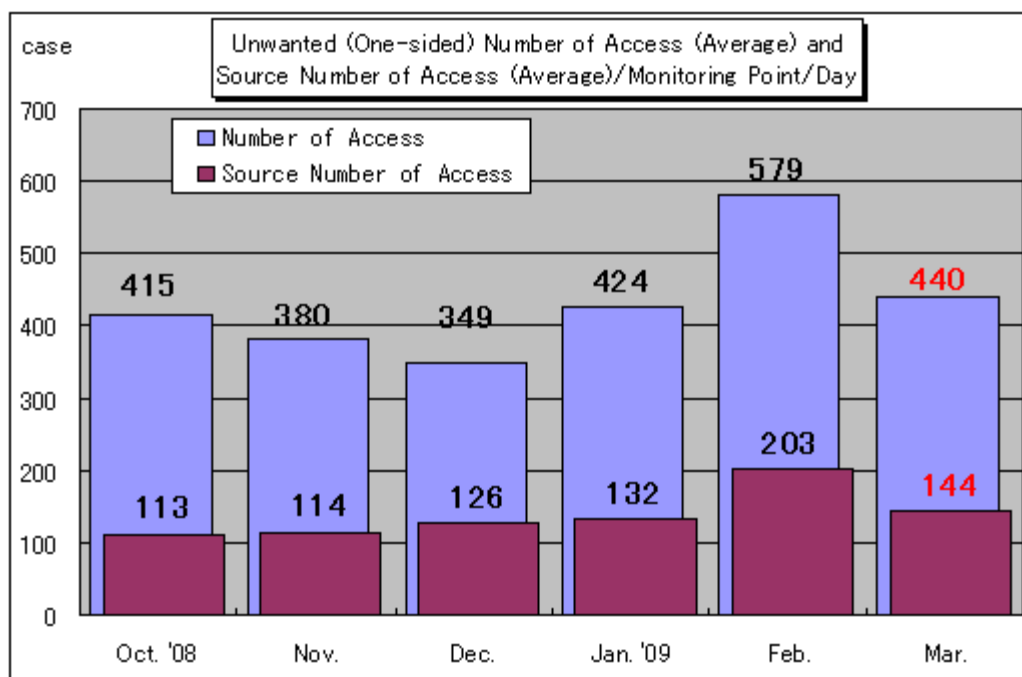


Chart 5-1: Unwanted (One-sided) Number of Access (Average) and Source Number of Access (Average)/Monitoring Point/Day

The Chart 5-1 shows the unwanted (one-sided) number of access and the source number of access (average)/monitoring point/day from October 2008 to March 2009. Both the unwanted (one-sided) number of accesses were drastically decreased from the ones in February.

(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 5-2). 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.

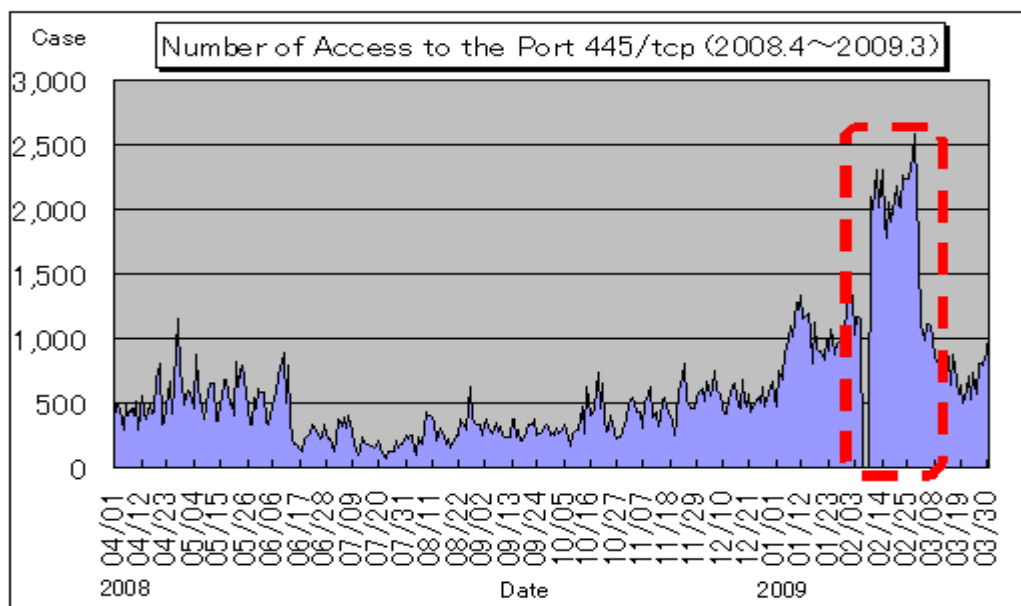


Chart 5-2: Shift in Number of Access to the Port 445/tcp Classified by Source Area

For more detailed information, please also refer to the following URLs.

Attachment_3: Accessing Status Captured by the Internet Monitoring (TALOT2)

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/TALOT2-0903.pdf>

Summary Reporting Status for Computer Virus/Unauthorized Computer Access for December

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/summary0903.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/virus0903.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/crack0903.pdf>

Variety of statistical information provided by the other organizations/vendors is available in the following sites.

@police: <http://www.cyberpolice.go.jp/english>

Trendmicro: <http://us.trendmicro.com/us/home/>

McAfee: <http://www.mcafee.com/us/>

Symantec: <http://www.symantec.com/>

Inquiries to:

Information-Technology Promotion Agency, Security Center

Hanamura/Kagaya/Ooura

Tel.: +81-3-5978-7527

Fax: +81-3-5978-7518

E-mail: isec-info@ipa.go.jp