

Computer Virus/Unauthorized Computer Access
Incident Report – August 2009

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

I. Reminder for the Month

“Isn’ t your Browser Being Hijacked?”
– Let’ s take immediate actions if unknown pages get to open automatically! –

As for current tendency, number of similar consultations like “Such windows for games and adult site (s) which I do not know get to open automatically upon booting up my computer and/or browsing web pages.” are rushed to IPA.

The malicious software to have your computer behaves differently is referred as “Browser Hijacker” in the sense as it hijacks Internet browsing software (hereafter refers as browser) such as Internet Explorer, etc. For here, we show you the process how your computer is infected by “Browser Hijacker”* as an instance and provide you some notes how and what things you have to be cautious with.

* Browser Hijacker is considered to be a sort of virus in a broad sense. For further details, please refer to (4) Countermeasures on page 4.

(1) What is “Browser Hijacker”?

Such malignant software that cause to have your computer displays unwanted/unexpected ads forcibly by altering the configuration for your browser or by adding fraudulent functions are referred as “Browser Hijacker”.

When your computer (i.e., browser) is hijacked by “Browser Hijacker”, following symptoms will be appeared.

- Such Tool Bar (*1) that you do not think you’d installed is added.
- Initial page to be displayed when your browser is booted is altered.
- Such ads or web pages you do not know get to open (pop-up) automatically.
- You are sent to malignant web pages automatically while you are browsing web pages.

Along with above mentioned symptoms, there identified such “Browser Hijacker” which also acts as “Spyware” which steals the archives you’d previously browsed and/or eavesdrops personal information such as your ID, password, etc (See the Chart 1).

(*1) The “Tool Bar” is a sort of function which helps to append the buttons for links to the Internet search engine and or variety of services on the upper part of your browser and is not necessarily a malignant. Of some are provided by Google, Yahoo!, etc. which enabling users accessibility and user-friendliness features.



Chart1: The Browser Hijacked by “Browser Hijacker” (Image)

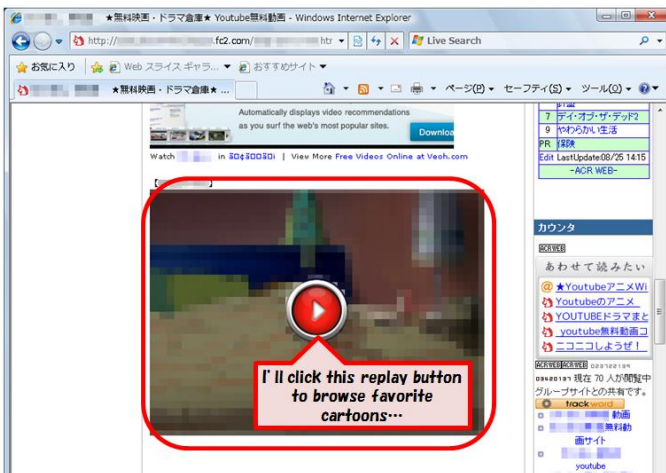
(2) Instance

For here, we provide you the infection mechanism by “Browser Hijacker” chronologically with the instance that “A computer hijacked by the “Browser Hijacker” when the user attempted to browse Japanese cartoons on an animation site”.



Step 1:

Using the key word (s), the user searches such URLs relevant to the cartoon (s) he/she wishes for by a search engine. Of the results listed, he/she chooses/clicks the links appeared on the upper portion of the search engine which seems to be “free” and “in Japanese”.



Step 2:

The site that the user jumped is the web site in where he/she may be able to browse the cartoon (s) he/she wishes for. As he/she scrolls the screen, somewhat a TV screen like area is appeared.

Well, let’s click the replay button in the center of the screen. Let’s see what cartoon will be served...



Step 3:

Soon after, a bigger window for animation which taking over the entire display screen is appeared.

Let’s click this replay button (?) like object one more time to see what’s going on here...

* To tell you the truth, this is a falsified screen masqueraded to be a window for animation to trap users: accordingly, “Browser Hijacker” will be downloaded regardless in where you’d clicked.

The actual window for animation (in the Step 2) is hidden by this bigger falsified screen.



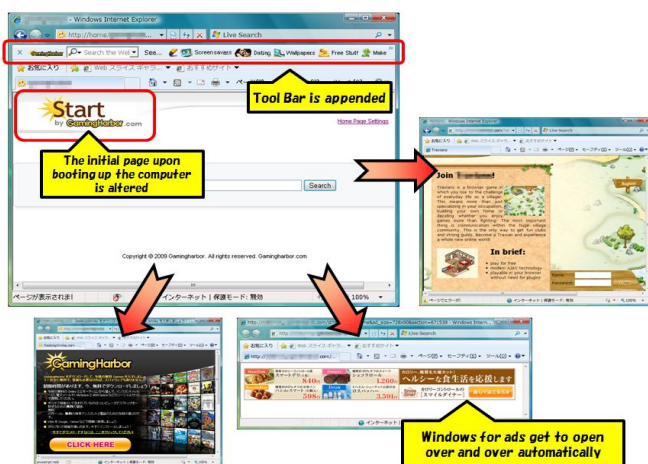
Step 4:

Any of cartoons is not replayed, but the smaller window for “Security Warning” is appeared, instead. The user easily clicks the “Run” button as he/she thought that he/she has to “Run” something to replay cartoons.

Well then, similar window is appeared again. The user again clicks the “Run” button anyway, but he/she does not realize what will be going on...

* We will further describe it later, but these windows are the important messages as they alert the user that some program (s) is downloaded.

This alert will not be appeared when you are simply browsing cartoons, so do not necessarily be worrying about.



Step 5:

The computer is infected by the “Browser Hijacker” by the operations described in the Step 4 above.

Such “Tool Bar” the user does not know is added and the initial page upon booting up the computer is altered.

In addition, (unwanted) game sites and/or windows for variety of ads get to open over and over automatically.

Though the computer behaves unnaturally in the Step 3 and 4 above; the user eventually infected by “Browser Hijacker” as he/she went to further (by clicking “Run”) carelessly. For here, we took up one of cartoon site (s) as an instance, but number of similar cases are also identified in drama, adult movie sites, etc.

Based on the scenario of “Browser Hijacker” above mentioned, following security issues can be considered.

- * Excessive trust for the URLs sequentially listed by a search engine
 - In this case, visiting the URLs at the upper portion listed by a search engine causes immediate damage. However, most of all users tend to believe that “Those web sites listed at the upper portion is enough secured”, accordingly, that they may not pay too much attention to the operations thereafter.
- * Security for the site linked is not viewable
 - Those web sites listed in the Step 2 above are just like “a series of links” to the variety of animation site being posted so that they do not ensure security. Actually, the animation player (enclosed with bold line in red) in the Step 2 is linked to the animation posting site (s) in overseas which conduct malignant activities such as displaying falsified screen to trap to users, etc.

* Security itself is hardly identifiable

- Since the falsified screen which traps users in the Step 3 is hardly distinguishable with the normal (i.e., sound) animation screen so that it is probable that number of users are fooled and click believing that this is the replay button for animation.

For your information, “Browser Hijacker” itself is not quite a newly emerged virus: “CooWebSearch” and “about: blank” (both are the virus names) are having been existed several years ago. The reason why the consultation number relevant to “Browser Hijack” tends to increase seemed that those users infected by this virus is increased via the infection mechanism above mentioned.

We will summarize the countermeasures the users can follow in the (3) and (4).

(3) What is “Security Warnings” Window?

We showed you the window so called “File Downloader – Security Warnings” in the Step 4 of the previous instance above. This is the window which alerts users that “your computer attempts to download program (s) from web site (s)” and provides 3 buttons such as “Run”, “Save” and “Cancel” the user can select from.

If you click “Run”, the program downloaded via web site (s) will be executed on your computer. As we described it previously in the instance above, your computer will be infected by virus if the program is malignant.

Unless those web site (s) you think you can enough trustful, you have to click “Cancel” button and do not go further when “Security Warnings” (window) is appeared. Though it seems that there is any of security matters in this program, you should download it on your computer any way and check it with your anti-virus software before open (execute) it for your further security.

Since the program developer is unknown, “Program Downloader – Security Warnings” also alerted in the instance above mentioned. Be sure to identify whether the program is enough trustful or not by its source, etc. before you click the “Run” button.

(4) Countermeasures

(i) Precautionary Measures

“Browser Hijacker” is one of viruses. Accordingly, its precautionary measures is exactly the same with the general anti-virus measures, such as:

- OSs and applications are to always up-to-dated.
- Install anti-virus software and maintain its signature file always up-to-dated.
- Use of such security software which helps to block malignant site (s).

As for general anti-virus measures, please refer to the following URL.

<Reference>

“The Tips How to Prevent Infection by Virus” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/personal/know/virus/html>

For your further information, “Browser Hijacker” may classify as one of adware, the software which purposes to forcibly display ads on the user’s screen. In case the user previously agrees to display ads, the “adware” is not considered to be malignant. Accordingly, some anti-virus software may not detect it as virus.

As we already described it in the (3) above, if every user can pay attention to the “Security Warnings” window, they may be able to prevent infection by virus. Be sure to remind “Security Warnings”.

As we explained it several times, the web site (s) (i.e., URLs) may not safe even they are in the upper portion of the results listed by a search engine (Even the web site (s) itself you are going to click is safe, but there may lay risky web site (s) which links to the site (s) you are going to click.).

With the users' knowledge, it is difficult to adequately determine the security of the site (s) by simply viewing the text written in a link (s), web page addresses (URLs), the aspects of the screen, etc.

Upon browsing web pages, it is helpful to leverage such software which provides "malignant site (s) blocking function^(*)" for your further security. They are effective as the users can display the security evaluation for the web pages linked, block to access to risky web site (s), etc. This blocking function is already provided as the part of the product so called "integrated anti-virus software".

As for Windows, such "malignant web site blocking function" so called "SmartScreen" is getting available from the Internet Explorer 8. As for how to use and their features, please refer to the following URL.

<Reference>

"SmartScreen Filter: Internet Explorer8 Readiness Toolkit" (Microsoft)

<http://www.microsoft.com/windows/internet-explorer/readiness/new-features.aspx#filter>

"SmartScreen Filter: Frequently Asked Questions" (Microsoft)

<http://windowshelp.microsoft.com/Windows/en-US/Help/184c6038-7eb1-4ca3-b50d-7901d81c37851033.msp>

(*) Since "malignant site (s) blocking function" is referred differently by respective providers such as "filtering (function)", "web reputation", etc.; for further details, please refer to the vendor/vendor's site for the security software you are using.

For your further information, here in IPA, we are providing such service that can diagnose/evaluate risks hiding in web site (s) on behalf of general users for their further security.

<Reference>

"Start to Provide General Users Web Site Information Using "Identification Information for Malignant Site and the System for their Countermeasures Information (TIPS)" (IPA) (in Japanese)

<http://www.ipa.go.jp/security/isg/tips.html>

(ii) Post Countermeasures

Of the "Browser Hijacker", there exists so malignant one that cannot remove with anti-virus software once it is infected. However, Windows XP and Windows Vista furnish "System Restoration" function so that you may be able to restore your system back to the state you were not infected.

<Reference>

"Using System Restore" (Microsoft)

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

What is System Restoration? – Windows Vista (Source: Microsoft "PC Talk") (in Japanese)

<http://support.microsoft.com/kb/934854/ja>

In case the system restoration was not successfully completed or your symptoms was not remedied, be sure to initialize your computer to the state it was initially purchased.

For your information, those computers once infected not only by "Browser Hijacker", but also by the other viruses may not be perfectly restored to the previous state: they can be seen that they are restored by anti-virus software and/or by system restoration function, anyway. Though data back-up and application re-configuration requires certain time, we encourage you to initialize your computer for your further security.

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

The detection number of virus (*1) in August was about **76T**: 4.9% decreased from about 8T in July. In addition, the reported number of virus (*2) in August was **1,222**: 2.7% decreased from 1,256 in July.

(*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 August, the reported number was 1,222 and the aggregated virus count was about 76T.

The worst detection number was for **W32/Netsky** with about **66T**: **W32/Mydoom** with about **4T** and **W32/Mytob** with about **2T** followed.

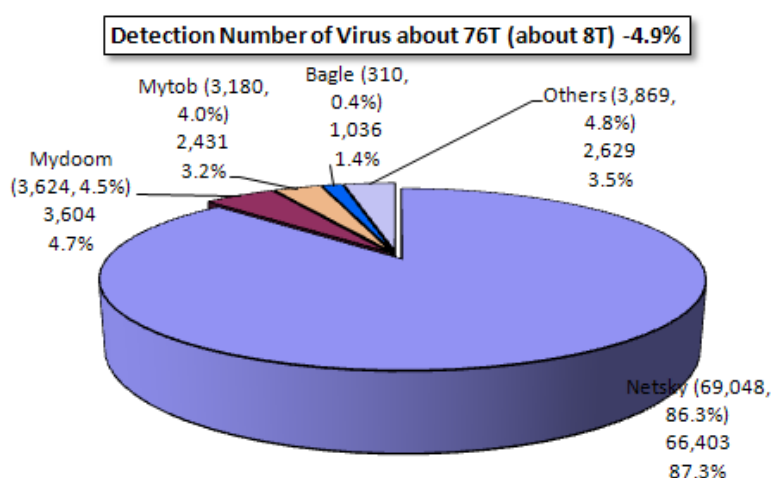


Chart 2-1: Detection Number of Virus

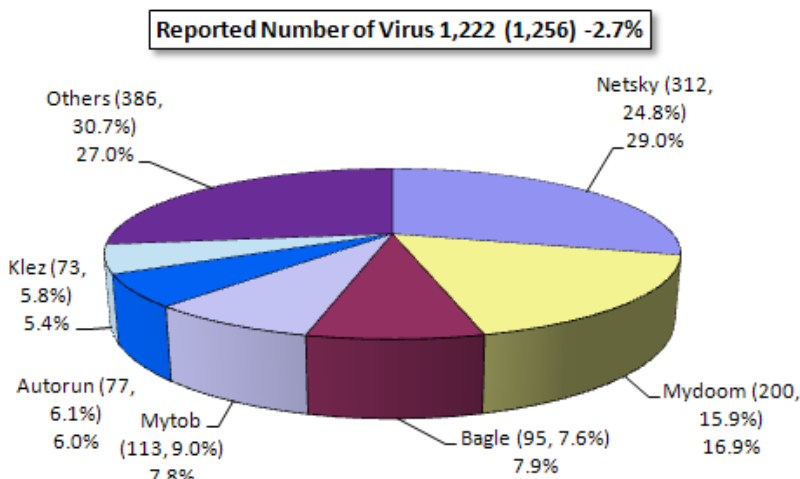


Chart 2-2: Reported Number of Virus

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

	Mar.	Apr.	May	June	July	Aug.
Total for Reported (a)	20	9	8	7	14	20
Damaged (b)	13	6	6	6	6	12
Not Damaged (c)	7	3	2	1	8	8
Total for Consultation (d)	40	39	45	35	24	39
Damaged (e)	11	11	16	9	3	17
Not Damaged (f)	269	28	29	26	21	22
Grand Total (a + d)	60	48	53	42	38	59
Damaged (b + e)	24	17	22	15	9	29
Not Damaged (c + f)	36	31	31	27	29	30

(1) Reporting Status for Unauthorized Computer Access

Reported number in August was **20**: Of **12** was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was **39** (of **6** were also counted as reported number): Of **17** was the number actually damaged.

(3) Status of Damage

The breakdown for damage reports included intrusion with **5**, masquerading with **5** and others (damaged) with **2**.

The damages caused by intrusion included: personal information theft within a web server such as credit number, etc. with 1, alteration of web pages (incl. embedding of malicious tags with 1) with 3, placement of malicious program with 1. The causes of intrusion were: insufficient configuration with 1, vulnerability was exploited with 1, insufficient password management with 1, etc. (the other causes have not yet been identified). The damage caused by “masquerading” was someone other than the legitimate user illegally logged in to the on-line service and then used this legitimate user-specific service (on-line game with 4, the other service with 1) without asking.

(4) Damage Instance

[Intrusion]

(i) Web page is altered by exploiting insufficient server configuration...

Instance	<ul style="list-style-type: none"> - Upon checking logs on web servers, suspicious access was identified. - Study was conducted: it was realized that the initial page of the web site was altered. - The cause was “FrontPage Server Extensions*” function exploited. - Since “FrontPage Server Extensions” is not necessarily need, we removed it from our web pages.
----------	---

*FrontPage Server Extensions: The tool to be appended to web server to extend FrontPage function, the web site construction tool by Microsoft

[Masquerading]

(ii) The service provided in a charged-animation distribution site (s) was used by someone without asking...

Instance	<ul style="list-style-type: none"> - I’d signed-up with a charged-animation distribution site, but I’d never used this service. The fee will be automatically charged to my credit card registered with the site. - One day, I was realized that the fees relevant to that animation distribution site which I do not know were charged to my credit card. - Accordingly, I inquired with the site: subsequently, it was realized that the IP address of the computer to which I’d accessed for the service (s) was not the one provided by the provider I am using. - The cause has not yet been identified.
----------	---

IV. Accepting Status of Consultation

The gross number of consultation in August was 1,792. Of the consultation relevant to “**One-click Billing Fraud**” was **654** (July: 657); this bad figure was maintained over the past 3 months. The consultation relevant to “**Hard selling of falsified anti-virus software**” was **1** (July: 6), the consultation relevant to “**Winy**” with **3** (July: 6), were also realized. (The consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” was **2** (July: 1).

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

	Mar.	April	May	June	July	August
Total	1,406	1,668	1,765	1,898	1,708	1,792
Automatic Response System	758	962	992	1,081	923	1,015
Telephone	597	651	710	777	736	702
e-mail	49	55	58	37	47	68
Fax, Others	2	0	5	3	2	7

*IPA consults/advises about computer viruses, unauthorized computer accesses, problems relevant to Winy 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, winy119@ipa.go.jp for emergent consultation relevant to Winy, 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. Reporting Status of Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

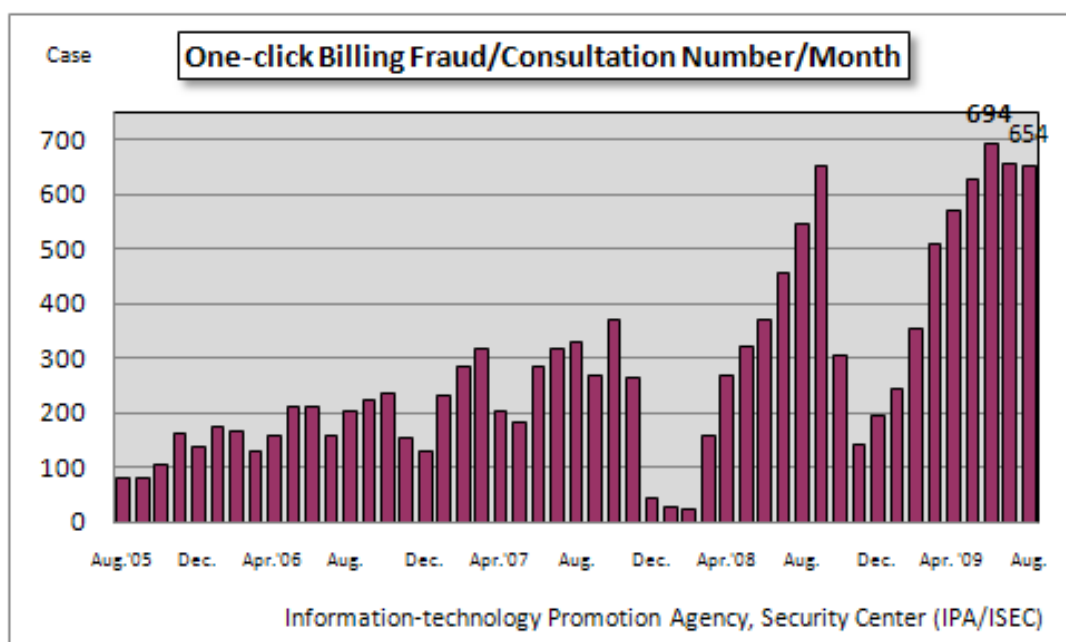


Chart 4-1: One-click Billing Fraud/Consultation Number/Month

The major consultation instances are as follows.

(i) Does the Anti-virus Measures for Corporate Network (Intranet) is Necessary...?

Consultation	My business has not installed any of anti-virus software in our computers. We do not feel necessity in security measures as we have never experienced the damage (s) caused by virus. In addition, it come to my ears that the computer behaves slower if anti-virus software would be installed, so we hesitate to do so. Are you sure that the software is necessary?
Response	<p>What if single private information deviation accident by virus is occurred, can you imagine how severely your corporate image, confidence in society would get damaged? It even jeopardizes business operation/managements. Everything is too late once you get damaged: accordingly, be sure to conduct at least fundamental security measures daily.</p> <p>For your information, any of latest versions of anti-virus software will not give too much burden on your computer (i.e., it does not consume too much memories, etc.). In addition, it may be of your help if you can eliminate unnecessary options.</p> <p><Reference> IPA – The Guidelines for IT Security Measures for Small and Medium Sized Businesses http://www.ipa.go.jp/security/fy20/reports/sme-guide/press.html</p>

(ii) I Got Damaged by “One-click Billing Fraud” When I was Searching the Information for Entertainment Personality...?

Consultation	When I was searching information relevant to one entertainment personality arrested with a search engine with her name as its keyword as I wanted to know the truth. Upon browsing some blog site (s) which seemed to be prepared by general users, I was caught by the words saying “Click here for spy photos”: When I clicked, I was sent to one of renowned animation posting sites like page. Accordingly, I clicked the replay button (?) provided in that page, then, such message “Thank you for your sign-up” is shown. Subsequently, a billing statement is getting appeared with several minutes of intervals.
Response	<p>It is probable that you are fooled by typical “One-click Billing Fraud”. The malicious person who conducts the fraud exploits variety of engineering to have his/her site be listed at the upper portion by a search engine: the one of methods is to prepare/distribute number of dummy site (s) that holds number of keywords which is relevant to current news everybody is interested in. To this end, general users tactfully be induced to malicious site (s) even those who do not purpose to browse adult site (s). The billing statement which appears several minutes of intervals is caused by virus. Users click it carelessly (most of users are likely to believe that it is the replay button for images/movies), but it is actually a virus infected by that computer: in the event, users download/implement virus by themselves. Since virus is malignant codes (program), Windows alerts “Security Warnings” when it is being downloaded. Users need to read the message what you are alerted and do not click the “Run” button carelessly to go further.</p> <p><Reference> IPA – Reminder for the Month (April 2009) “Do you know about Security Alert Screen?” http://www.ipa.go.jp/security/english/virus/press/200903/E_PR200903.html</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in August was **171,271** for the 10 monitoring points and the gross number of source* was **65,738**. That is, the number of access was **552** from **212** source addresses/monitoring point/day.

*Gross number of source: Gross number of source refers the total of source number of access summed-up to the respective monitoring points in TALOT2.

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.

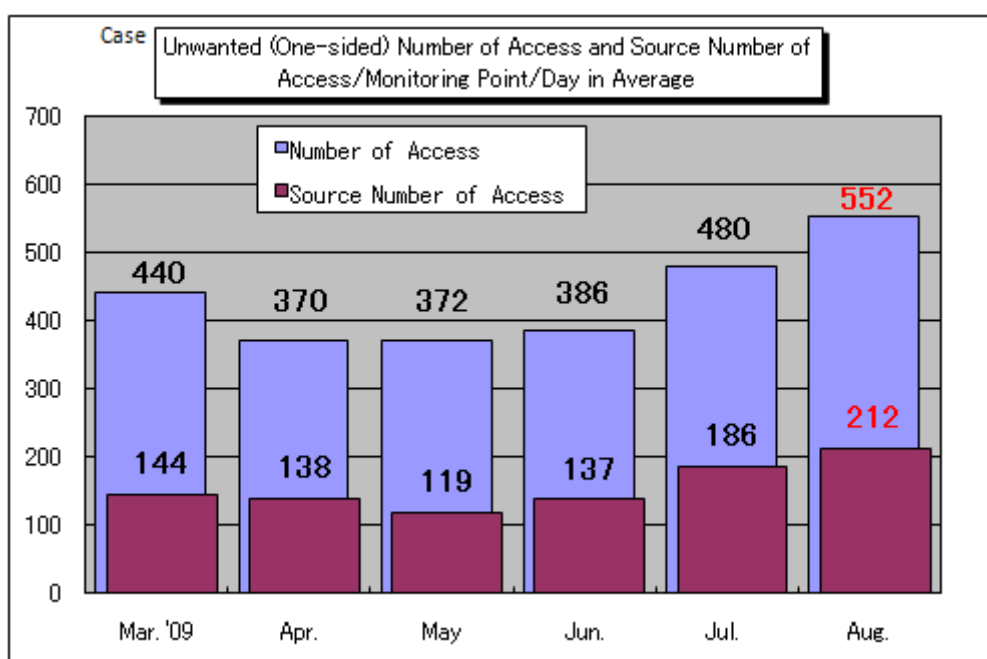


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day in average from March to August 2009. Both the unwanted (one-sided) number of access and the source number of access were increased compared with those in July.

The Chart 5-2 shows the comparison in the number of access classified by the destination (by port) in July and August. The number of access significantly increased in August was the access to the port 445/tcp. Though the number of access from specific source was not increased, the entire number of access was increased by the number of access to the port 445/tcp. In August, the number of access to the port 39023/tcp which had never been monitored in July could be observed frequently. We cannot identify what did this access purpose for: this access was only monitored at single monitoring point.

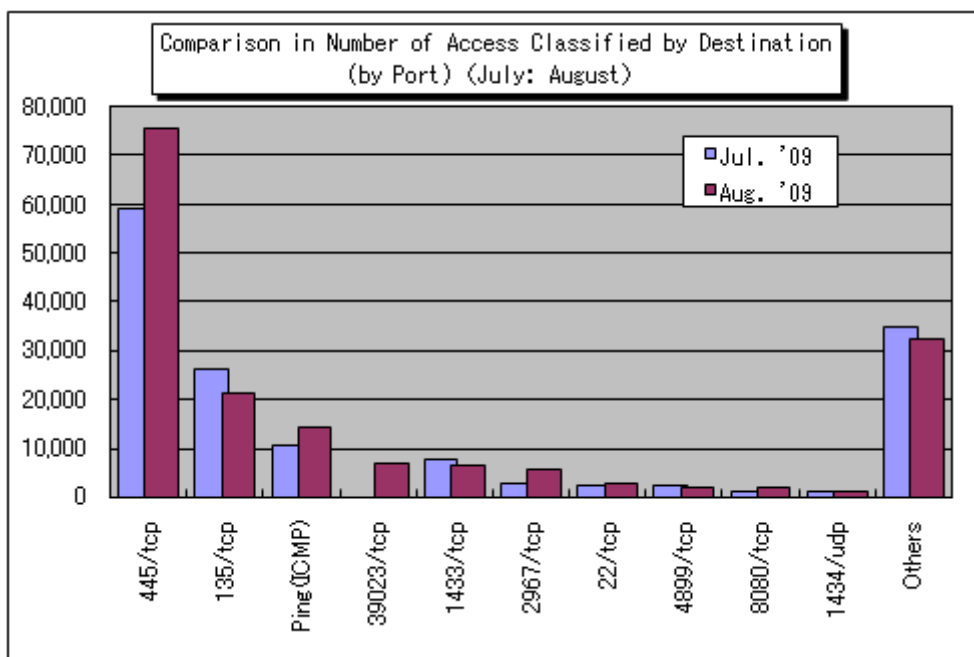


Chart 5-2: Comparison in Number of Access Classified by Destination (by Port) (July: August)

As you can see the Chart 5-1, the number of access/monitoring point/day in average tended to gradually increase over the past 4 months. The Chart 5-3 shows the shift in number of access to the top 10 ports (i.e., the worst 10 ports) frequently accessed over the past 4 months.

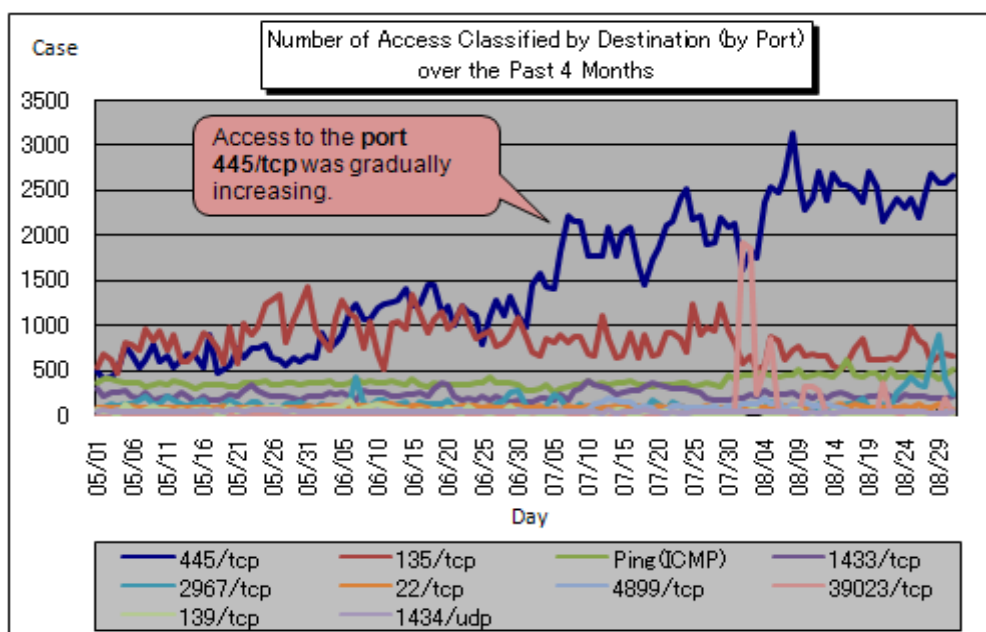


Chart 5-3: Number of Access to the Port 445/tcp Classified by Destination (by Port) over the Past 4 Months

According to this chart, while the number of access to the most of all ports was shifted by maintaining certain level, yet the number of access to the port 445/tcp was gradually increasing; it can be seen that the access to this port affected to the entire number of access (in average) significantly.

Since the port 445/tcp was renowned as the port to be exploited when conducting attacks targeting vulnerability in Windows; however, the cause why it has been increasing and been monitored by the TALOT2 for such a long period has not yet been identified.

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/200908/documents/TALOT2-0908.pdf>

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

<http://www.ipa.go.jp/security/english/virus/press/200908/documents/summary0908.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200908/documents/virus0908.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200908/documents/crack0908.pdf>

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

JPCERT/Coordination Center (CC): <http://www.jpccert.or.jp/english/>

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

Council of Anti-Phishing Japan: <http://www.antiphishing.jp/>

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

Trendmicro: <http://www.trendmicro.com/en/home/us/home.htm>

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

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