

Computer Virus/Unauthorized Computer Access Incident Report – June 2009

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

I. Reminder for the Month

“Isn’t Your Website being Altered?”

– Your website may have been tailored as such website spreading virus –

Currently, there emerged that the number of instances that those websites operated by businesses and individual users are being altered. In the websites being altered, there may be embedded such traps to have users who browsed that websites to infect virus. In the event, there rushed number of reports and consultations to IPA such that “virus was detected”, “computer was infected by virus”, etc. from the users whose websites were being altered.

Such website manager whose website was being altered supposed to be a casualty; however, he/she will also be a victimizer to have the other users’ computers infect virus. To prevent enlarging such damage, website manager should check if his/her website is not illegally altered to the “hub to spread virus”.

(1) Website Alteration – the Overview and the Major Cause

As for the cause of website alteration, there is the instance that the account information for ftp* was stolen. In that instance, a malicious intent used the ftp account (ID/password) stolen to masquerade to be a legitimate user and whose web pages altered were publicized (i.e., uploaded) on the web server.

As for the methodology to steal ftp account, sending spyware to subjected computer is often used.

*File Transfer Protocol: such protocol to transfer files via a network.

In the web pages being altered, there embedded fraudulent scripts: accordingly, those general users who’d browsed that pages automatically send to the malicious site in where certain virus was trapped. What if the general user browses that malicious website, he/she will be infected by virus if there is vulnerability in his/her computer (see the Chart 1-1).

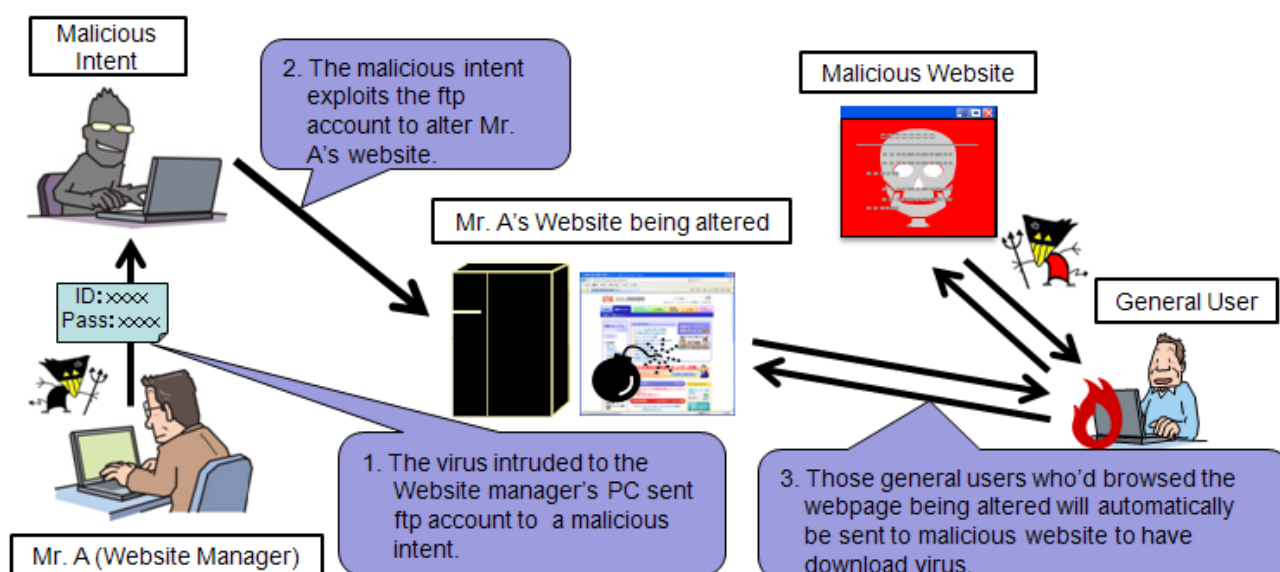


Chart 1-1: The Mechanism from Web Alteration to Virus Infection

Though repeatedly altered with the same method in vain even you'd changed your password, it is possible that your computer used to change the password may be infected by spyware and the important information such as your ftp accounts, etc. may have been deviated. Accordingly, when you change your password to re-publicize your website, be sure to clean up (i.e., initialize) your computer to free from fraudulent program in advance.

It is ideal to eliminate the cause (s), modify the web pages altered, and then re-publicize the website in turn in case your website is being altered. We also encourage those website managers for whom websites were being altered should communicate their users the facts that your website was altered; there may have been certain risks to get infected by virus and apologize those users who'd browsed your website previously via your renewed website as well. For your further information, it is also ideal to provide inquiry window for general users.

In addition, in case you get damage (s) such as your website is altered; your computer is infected by virus; etc.: be sure to file them with IPA as possible as you can. Here in IPA, we accept reports relevant to both virus and unauthorized computer access: we parse such reports for statistical purposes and publicize them other than the information which is identifiable certain person or business on our website monthly. The reports are also leveraged when we publicize information relevant to countermeasures against viruses, unauthorized computer accesses, etc.

<Reference>

“Reports relevant to Information Security” (IPA)(in Japanese)

<http://www.ipa.go.jp/security/todoke/>

(4) Measures should be taken by Users

In case a user infects virus by browsing the web pages being altered, it will be the significant threat if he/she cannot realize virus infection visually as there displays none of anomaly. Further, there is number of cases that none of specific symptoms is appeared visually in case infected.

To prevent such virus infection, be sure to conduct following measures.

(a) Resolve vulnerability (ies)

There identified vulnerability (ies) in OSs such as Windows and Mac OS, in application software such as Microsoft Office, Adobe Reader, etc. Be sure to resolve vulnerability (ies) by update your OSs and applications to the latest version, by applying patches, etc.

<Reference>

“JVN iPedia The Database for Anti-Vulnerability Measures Information” (JVN)

<http://jvndb.jvn.jp/en/>

(b) Anti-virus measures

Be sure to update your signature for your anti-virus software regularly to have your virus detection function always effective.

(5) The Symptoms upon Infected by Virus

When infected by virus in the event that you'd browsed the website being altered and automatically sent to a malicious site, your computer may show following symptoms.

- Cannot resolve vulnerability since access to the Microsoft Update is interfered.
- Information relevant to virus is not available, cannot update virus signature, etc. since the site (s) for security measures software vendors is not accessible.
- Cannot run command prompt (cmd.exe) and/or registry editor (regedit.exe).

When such symptoms are identified, it is probable that your computer is infected by virus. There may be a case that your computer is infected by several viruses at one time. To fully remove the viruses, you are to initialize your computer: be sure to back up necessary data files to certain removable memory media such as USB memory, etc. before you start to initialize

your computer.

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

The detection number of virus in June was about 87T: 24.4% decreased from about 115T in May. In addition, reported number of virus in June was 1,460: 5.3% increased from 1,387 in May.

(*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 June, the reported number was 1,460 and the aggregated virus count was about 87T.

The worst detection number was for W32/Netsky with about 70T; W32/Downad with about 6T and VBS/Solow with about 3T subsequently followed.

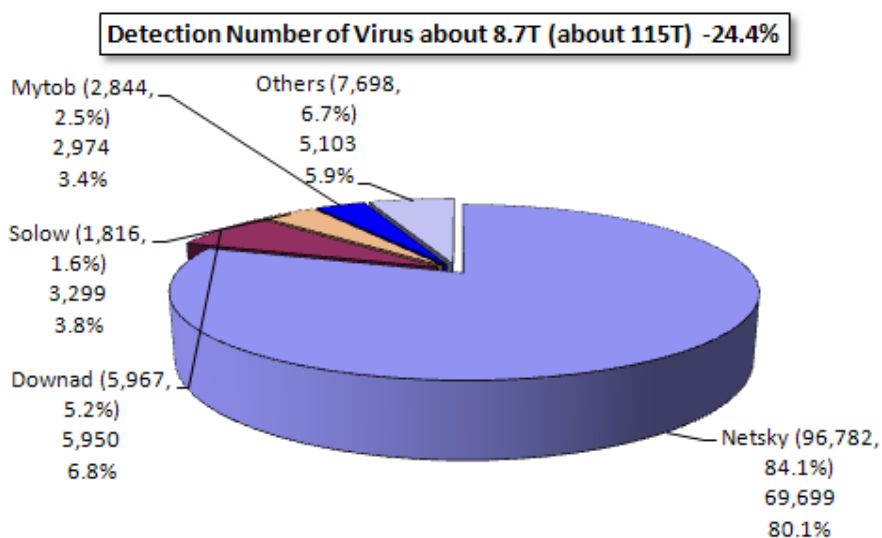


Chart 2-1: Detection Number of Virus

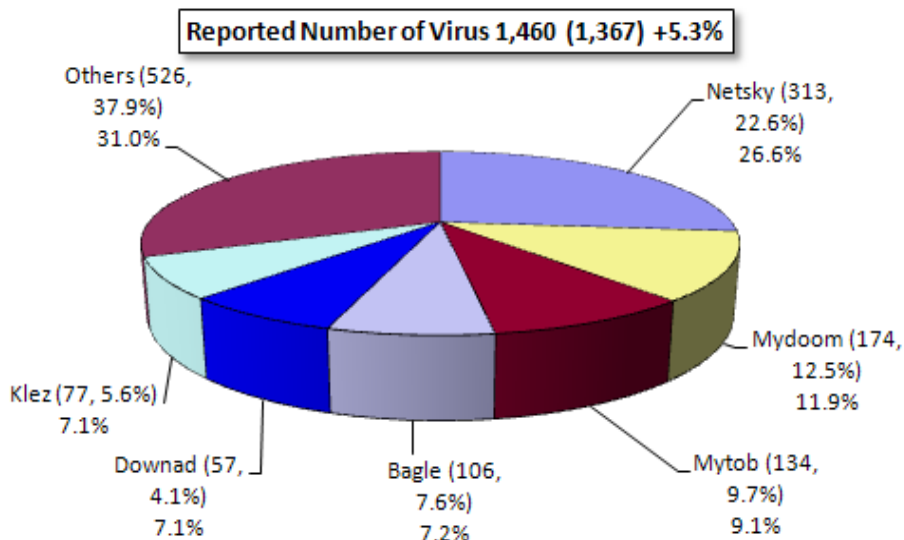


Chart 2-2: Reported Number of Virus

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

	Jan. '09	Feb.	Mar.	Apr.	May	June
Total for Reported (a)	10	9	20	9	8	7
Damaged (b)	7	6	13	6	6	6
Not Damaged (c)	3	3	7	3	2	1
Total for Consultation (d)	29	35	40	39	45	35
Damaged (e)	13	14	11	11	16	9
Not Damaged (f)	16	21	269	28	29	26
Grand Total (a + d)	39	44	60	48	53	42
Damaged (b + e)	20	20	24	17	22	15
Not Damaged (c + f)	19	24	36	31	31	27

(1) Reporting Status for Unauthorized Computer Access

Reported number in June was 7: Of 6 was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was 35 (of 1 was also counted as reported number): Of 9 was the number actually damaged.

(3) Status of Damage

The breakdown for damage reports included intrusion with 1, DoS attack with 1, masquerading with 3 and embedding of fraudulent program with 1.

As for the damages caused by intrusion was that the server was exploited as a steppingstone server to attack to the other site (s). The cause of intrusion was that the server was conducted by password cracking* attack to the ports used by SSH*.

- * SSH (Secure Shell): One of the protocols to communicate with the computer remotely via a network.
- * Password Cracking: The activity to analyze/parse the other person's password illegally. Brute Force Attack (Exhaustive Search Attack) and Dictionary Attack are the well-known methods. The program for cracking activity is also existed.

(4) Damage Instance

[Intrusion]

- (i) Conducted by TCP SYN Flood attack and the service to be provided for customers is getting unavailable...

Instance	<ul style="list-style-type: none"> -In the business which carries on rental servers and ASPs, all the services provided for customers are suddenly getting unavailable as the firewall was significantly overloaded. -Study was conducted: it was realized that the server was conducted by TCP SYN Flood attack so that about 100 million of packets were accessed about every 30 minutes. -Accordingly, those IP addresses for the targeted server were temporarily changed; however, it was again realized that the packets were started to access to the newer IP addresses shortly. -The client's domain for the targeted IP address assigned to the rental server was more than 100 so that we squeeze/narrow down the targeted domain, we eventually identified that the RMT (real money trading) site (s) relevant to online games were targeted. -Then we temporarily manipulated "A" record of DNS in the targeted domain to block to the packet not to reached within the firewall (i.e., inside the organization). It seemed that the attack had been conducted for two (2) days in total.
----------	---

* TCP SYN Flood Attack: The one of the DoS attacks which exploits TCP protocol to lower and/or to halt server's function.

[Masquerading]

- (ii) Deceived and stolen my password at an online game site...

Instance	<ul style="list-style-type: none"> -Someone identifies him/herself as the site manager for the online game site requested me to chat when I was playing games at that site. -I responded to it as I assumed that the site manager is patrolling within his/her site. I'd given my ID and password as I was requested to authenticate my identification. -Soon after my ID and password were altered/hijacked.
----------	--

IV. Accepting Status of Consultation

The gross number of consultation in June was 1,898. Of the consultation relevant to “**One-click Billing Fraud**” was **694** (May: 628): the number was getting worsened ever. The consultation relevant to “**Hard selling of falsified anti-virus software**” was **6** (May: 2), the consultation relevant to “**Winny**” with **13** (May: 5), were also realized. (The consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” was **0** (May: 5).

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

	Jan. '09	Feb.	Mar.	Apr.	May	Jun.
Total	960	1,051	1,406	1,668	1,765	1,898
Automatic Response System	529	521	758	962	992	1,081
Telephone	390	472	597	651	710	777
e-mail	39	57	49	55	58	37
Fax, Others	2	1	2	0	5	3

*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”.

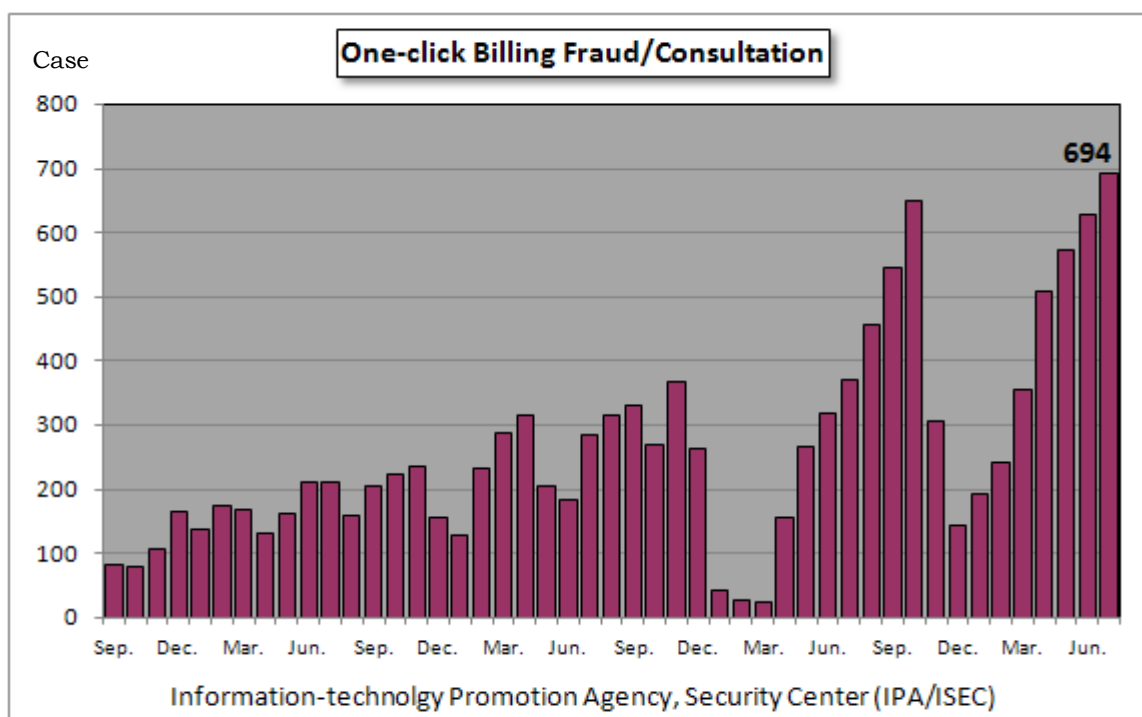


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

- (i) I may not be infected by virus even I do not update my OSs as I am installing anti-virus software...?

<p>Consultation</p>	<p>I am using Windows 2000 and Windows XP in my business. Anti-virus software is installed and their signature files are always up to dated so that I may not be infected by virus even I do not conduct Windows Update?</p>
<p>Response</p>	<p>That concept is not true. You may have high risk to get infected by virus if the vulnerability in your computer is not resolved by Windows Update, etc. Hereafter, we explain it allegorically.</p> <p>PC as in ... a house (physical building) Anti-virus software as in ... the entity that monitors in- and out-bound accesses from the door/window for the house (physical building)</p> <p>For here, such condition that the Windows Update is not conducted mean to be the “house that has certain failure”: it can be assumed that “the wall was partially/entirely collapsed”, “the roof has big hole (s)”, etc. That is, if vulnerability is remained, someone (malicious intent) can easily be intruded into your house with insane attempts.</p> <p>Resolving vulnerability is the fundamental security measures.</p> <p><Reference> Seven Rules of Virus Countermeasures for PC Users (IPA) http://www.ipa.go.jp/security/english/virus/antivirus/7RulesV.html</p>

- (ii) Even Windows 98 and Me are safe if I do not connect to the Internet...?

<p>Consultation</p>	<p>I have a Windows 98 based computer. I have not used it awhile, but I wish to use it again as a word processor or a spreadsheet purposes hereafter. I will not have any risk (s) to get infected by virus if I will not connect to the Internet or a domestic LAN?</p>
<p>Response</p>	<p>Even unconnected, there remains certain risk (s) to get infected by virus if you will exchange some data with the other PC (s). Nowadays, there spreading such virus which infects via an USB memory so that you have to specifically pay attention to it. As for Windows 98/Me, their supporting period by Microsoft is already terminated so that the modification program (s) will not be provided even vulnerability will be developed thereafter: you are confronting high risk (s) accordingly. Even your anti-virus software can respond to it, the anti-virus function may not be properly operated as the OS itself carries problems. That is, if you use such OS for which supporting period is terminated, you have to use it with defenseless state. Naturally, your PC is remained to be risky, so that we do not recommend to use those OSs for which supporting period by its manufacturers is terminated.</p> <p><Reference> Seven Rules of Virus Countermeasures for PC Users (IPA) http://www.ipa.go.jp/security/english/virus/antivirus/7RulesV.html</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in June was **115,860** for the 10 monitoring points and the gross number of source* was **41,065**. That is, the number of access was **386** from **137** 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.

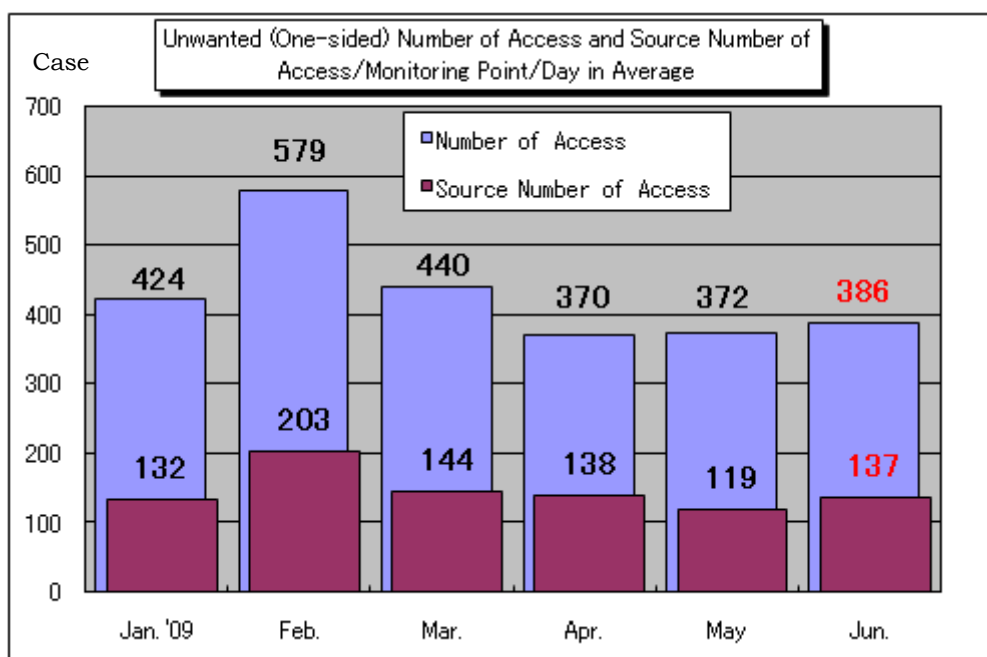


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day from January to June 2009. Both the unwanted (one-sided) numbers of accesses were subtly increased compared with the ones in May.

The Chart 5-2 shows the comparison in numbers of access classified by destination (by port) for the months of May and June.

In June, the number of access to the port 445/tcp was significantly increased since the access to that port from overseas was increased compared with the one in May (See the Chart 5-3). The cause why such access from overseas was increased has not yet identified; however, the number of access from specific source was not increased, but the entire source number of access from overseas itself was directly relevant to that increase.

In addition, we'd obtained such information that the access to the port 445/tcp from overseas was increased from the other organization who also conducts the Internet monitoring.

As for the other ports other than the port 445/tcp were not significantly shifted, but the accesses to the ports other than the worst 10 ports were significantly decreased.

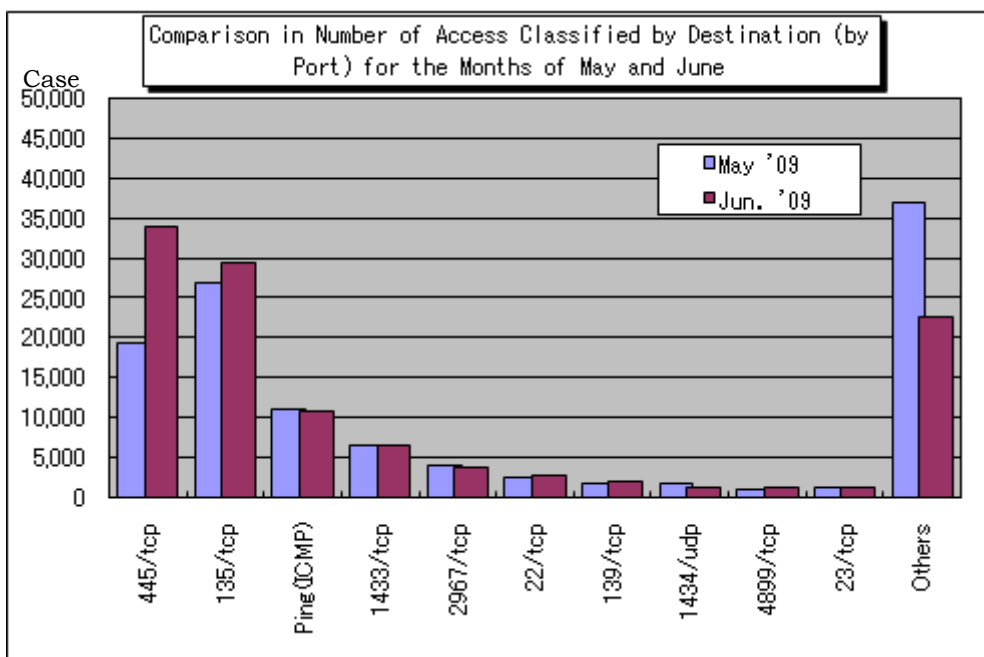


Chart 5-2: Comparison in Number of Access to the Port 445/tcp Classified by Destination (by Port) for the Months of May and June

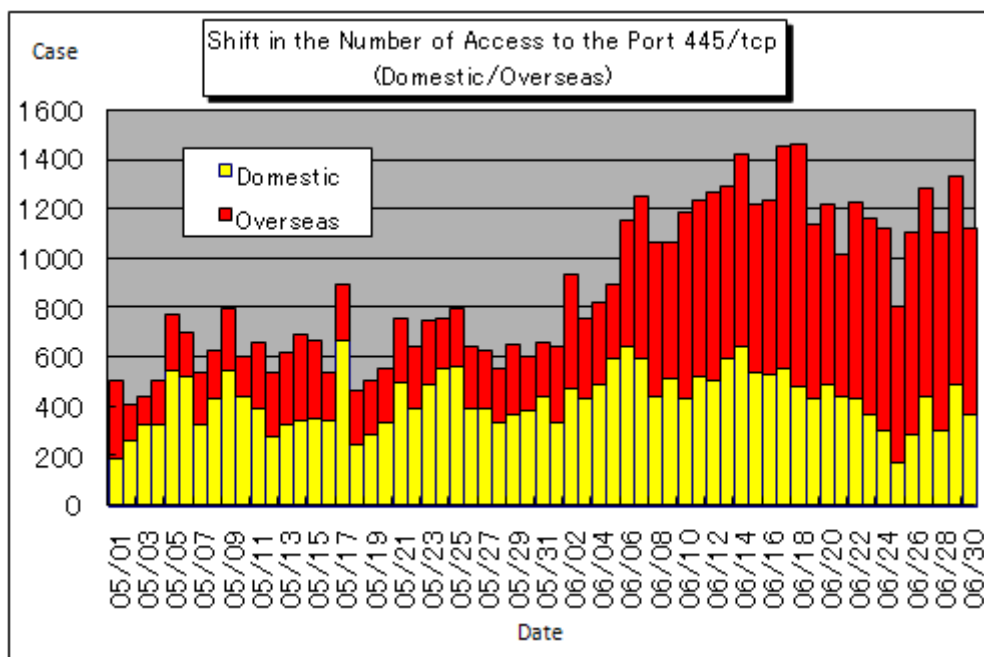


Chart 5-3: Shift in Number of Access to the Port 445/tcp (Domestic/Overseas)

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/200906/documents/TALOT2-0906.pdf>

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

<http://www.ipa.go.jp/security/english/virus/press/200906/documents/summary0906.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200906/documents/virus0906.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200906/documents/crack0906.pdf>

Attachment_4 Computer virus Incident Report for the 1st Half (April to June)

<http://www.ipa.go.jp/security/english/virus/press/200906/documents/virus2009-1H.pdf>

Attachment_5 Unauthorized Computer Access Incident Report for 1st Half (April to June)

<http://www.ipa.go.jp/security/english/virus/press/200906/documents/ua2009-1H.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