

Computer Virus/Unauthorized Computer Access Incident Report – July 2009

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

I. Reminder for the Month

“Do You Know about ZERO-DAY ATTACK?”
– Be sure to comprehend the principles of anti-vulnerability measures –

Here in IPA, we analyze the vulnerability information provided by software providers (vendors): we alert of the consequences deemed to be important/urgently be handled as the vulnerability alert on our official website. In July, there released 4 vulnerability relevant information from Microsoft and 1 from Adobe Systems: we alert of 3* as the security alert since there identified such attack (s) exploiting the said vulnerability (ies) in prior their modification program would be provided by respective vendors.

As you are already aware that responding them (i.e., applying them to your computer) promptly as soon as they are released is the principle of anti-vulnerability measures; however, as we mentioned it above, their modification program may have not been available at that time. In that case, it is important to check relevant information/relevant site (s) as possible as you can: there may be provided alternative/tentative measures.

Be sure to comprehend the principles of anti-vulnerability measures properly to protect your computer from the attack (s) like the one described above.

* "Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (971633) (MS09-028)", "Cumulative Security Update of ActiveX Kill Bits (973346) (MS09-032)" and "Vulnerability in Adobe Reader, Acrobat and Adobe AIR".

(1) What is “Vulnerability”?

Security relevant weakness on OSs and application software for Windows and Mac OSs, etc. refer to be “vulnerability”. What if vulnerability is not resolved, you may get damage when your computer would be attacked exploiting that vulnerability. The principle of anti-vulnerability measures against such attack is to resolve the vulnerability by applying their modification programs.

IPA has been recommending two items as fundamental/major security measures: resolving of vulnerability and maintaining of anti-virus software always up-to-dated. What if you conduct either one of these, you cannot expect sufficient effects: they will work out only when you apply both of them in concert. Even you always up-to-date your anti-virus software, it is likely that you would allow intrusion from outside illegally if you do not resolve vulnerability (ies) (See the Chart 1-1).

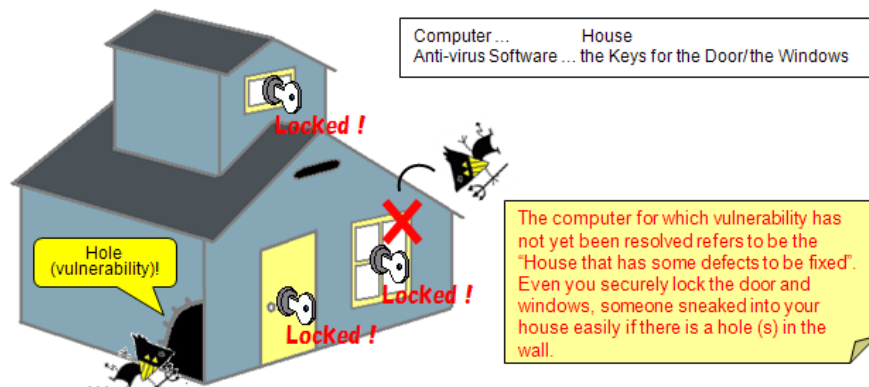


Chart 1-1: Vulnerability can be Referred to be the Hole in a House (Computer)

(2) What is “Zero-Day Attack”?

The attack (i.e., access) exploiting vulnerability in software before its modification program is getting available refers “Zero-Day Attack”: they are the attack (s) specifically identified/conducted in the period that the said modification program is not yet provided by the subjected software vendor (s) (See the Chart 1-2).

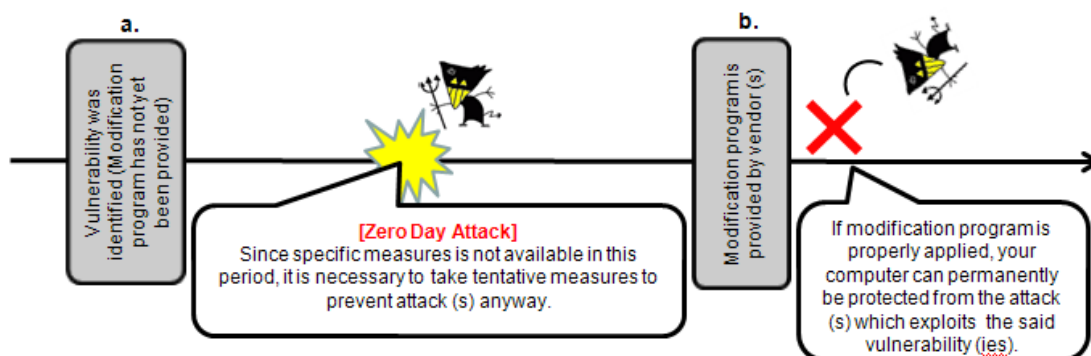


Chart 1-2: “Zero-Day Attack”

Follows, we further describe the “Zero-Day Attack” with the “Cumulative Security Update of ActiveX Kill Bits (973346) (MS09-032)” identified in July as its specific instance.

<Chronological>

[Specific time and date were not identified]

The attack which exploits the said vulnerability was caused (a. in the Chart 1-3).

[July 6, 2009 (in U.S. time)]

The attack which exploits the said vulnerability was identified: vulnerability alert relevant to “Cumulative Security Update of ActiveX Kill Bits (MS09-032)” was publicized by Microsoft. Though the modification program was not available at that time; tentative measures against the attack was provided (b. in the Chart 1-3).

[July 14, 2009 (in U.S. time)]

The vulnerability alert relevant to MS09-032 was up-to-dated and its modification program was provided by Microsoft (c. in the Chart 1-3).

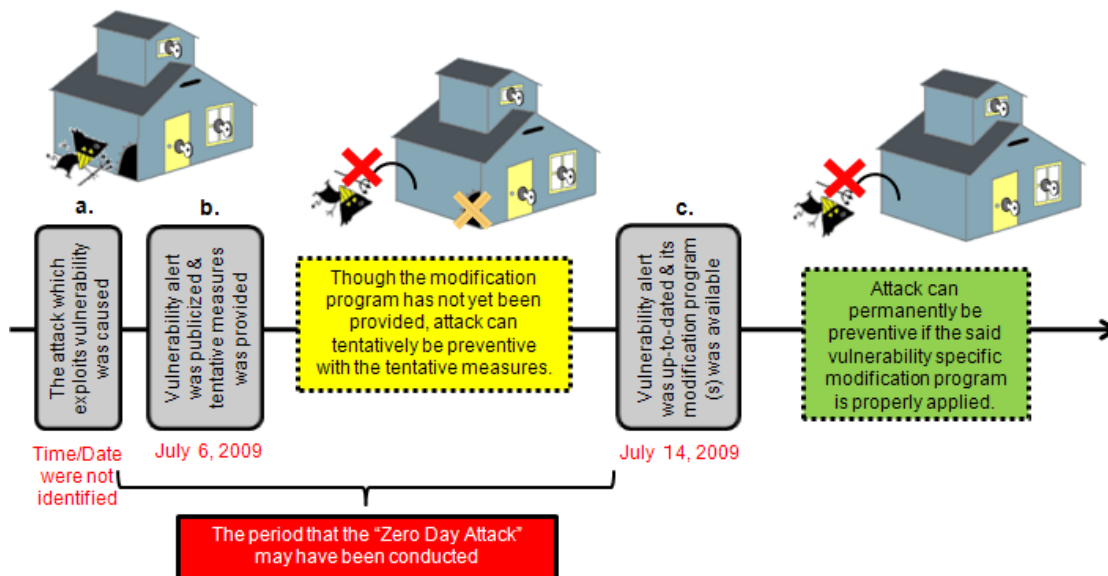


Chart 1-3: Chronological Responses against the Vulnerability (MS09-032)

As with the instance above (MS09-032), the attack which exploits the said vulnerability was identified before the vulnerability-specific measures were publicized (a. in the Chart 1-3). The user could prevent attack (s) if he/she would promptly conducted tentative measures with the vulnerability alert publicized by Microsoft on July 6 any way and then subsequently applied the vulnerability-specific modification program upon the vulnerability alert was updated on July 14.

However, those users who did not even know that the vulnerability specific information was publicized may have been attacked as they have missed the chance to conduct even the tentative measures against that vulnerability.

For your further security, be sure to conduct the measures relevant to the subjected “Zero-Day Attack” by referring to the notes provided in the next section.

<Reference>

“Microsoft Security Advisory (972890)” (Microsoft)

<http://www.microsoft.com/technet/security/advisory/972890.mspx>

“Microsoft Security Bulletin MS09-032 - Critical” (Microsoft)

<http://www.microsoft.com/technet/security/bulletin/ms09-032.mspx>

“Security Alert relevant to the vulnerability in Microsoft Video ActiveX Control (MS09-032) (IPA) (in Japanese)

<http://www.ipa.go.jp/security/ciadr/vul/20090707-ms-activex.html>

(3) Notes how to prevent from “Zero-Day Attack”

To prevent from “Zero-Day Attack”, it is important that every user is to comprehend the vulnerability information publicized by respective vendors and to address them adequately. “Vulnerability alert” by IPA, the portal site for “vulnerability information” such as JVN, etc. are also helpful. As with the instance in the (2) above, tentative measures may have been available even the vulnerability specific modification program was not provided upon the publication of vulnerability information. However, some tentative measures may lead specific services unavailable; it is necessary to be cautious when you conduct them, accordingly.

In case tentative measures were not provided, you should better not to use the subjected software awhile: be sure to apply vulnerability specific modification program is officially available, as soon as they are released, accordingly. As we mentioned above, to address the vulnerability properly, it is important to collect relevant information daily. In addition, it is also important to maintain your anti-virus measures software always up-to-dated.

Follows are some of effective methods to collect information referable for your anti-vulnerability measures.

(i) Information collection via mail magazine

Vulnerability relevant information can be obtained easily from the security software vendor for the OSs and/or application software and/or computer manufacturer you are using if they provide information via their mail magazine. If you are a Microsoft user, you can be a subscriber via the following URL.

For your information, IPA alerts “vulnerability alert” on our website for those vulnerability information publicized by respective vendors that deemed to be emergently addressed as the consequence (s) analyzed by us. We distribute our subscribers the “vulnerability alert” as well.

<Reference>

“Security Newsletter” (Microsoft)

<http://technet.microsoft.com/en-us/security/cc307424.aspx>

“Newly Arrived Information” (IPA) (in Japanese)

<http://www.ipa.go.jp/about/mail>

(ii) Information collection via websites

Vulnerability relevant information may be obtained from the security software vendor for the OSs and/or application software and/or computer manufacturer you are using on their websites so that we recommend you to visit their homepage regularly. If you are a Microsoft user, following URL can be helpful.

Of the vulnerability information publicized by respective vendors, IPA alerts “vulnerability alert” for those that deemed to be urgently handled as the consequence (s) from the analytical review on our website. Vulnerability relevant information for the software used in domestic and the JVN, the portal site for vulnerability information, etc. can also be referable.

<Reference>

“Security – TechCenter” (Microsoft)

<http://technet.microsoft.com/en-us/security/default.aspx>

“security at home” (Microsoft)

<http://www.microsoft.com/protect/default.msp>

“SECURITY ALERTS” (IPA)

<http://www.ipa.go.jp/security/english/securityalerts.html>

“JVN (Japan Vulnerability Notes)”

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

(iii) Supplementary articles/interpretations

You can also refer to the articles on the news site (specifically in the IT industry) and/or relevant information on the portal site (s) as well. You may acquire effective/helpful information as there may be publicized vulnerability relevant information.

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

The detection number of virus (*1) was about 80T; 14% decreased from 87T in June. In addition, the reported number of virus (*2) in July was 1,256; 8% decreased from 1,460 in June.

(*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 July, the reported number was 1,256 and the aggregated virus count was about 80T.

The worst detection number was **W32/Netsky** with **about 70T**; **W32/Mydoom** with **about 4T** and **W32/Mytob** with **about 3T** subsequently followed.

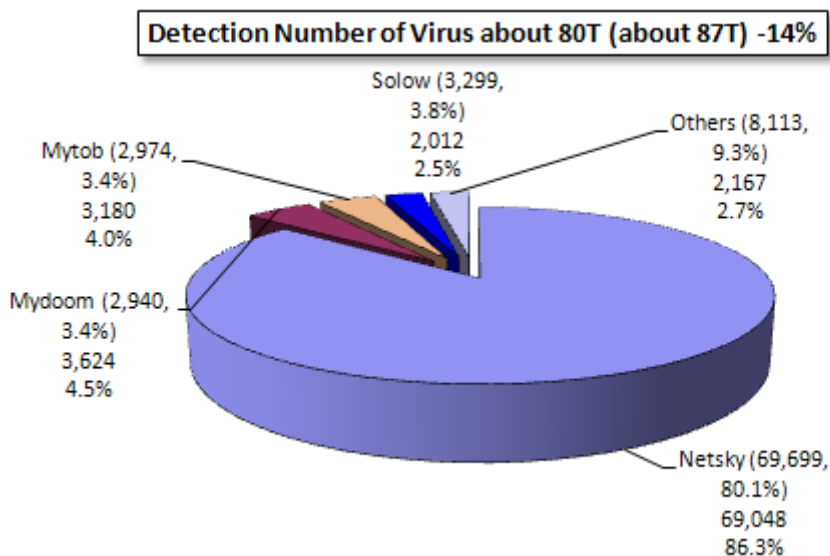


Chart 2-1: Detection Number of Virus

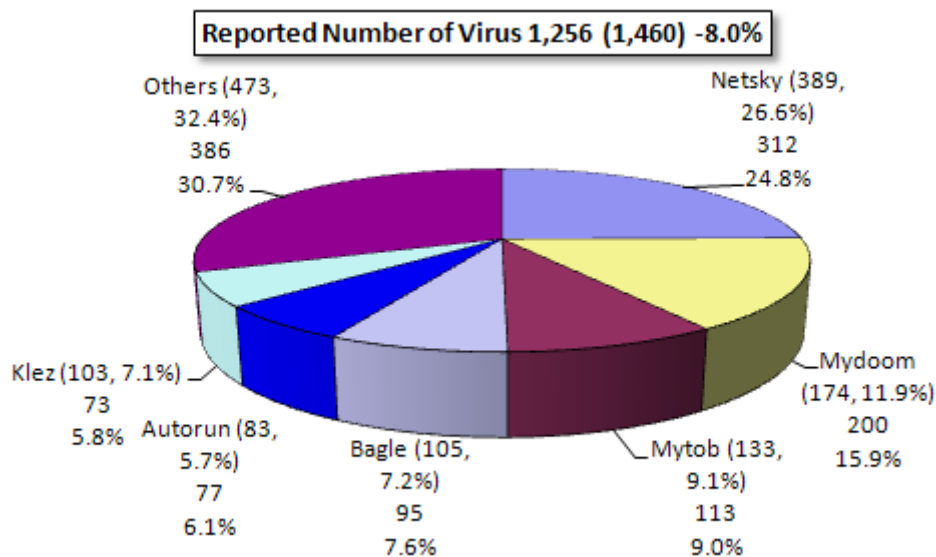


Chart 2-2: Reported Number of Virus

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

	Feb.	Mar.	Apr.	May	Jun.	Jul.
Total for Reported (a)	9	20	9	8	7	14
Damaged (b)	6	13	6	6	6	6
Not Damaged (c)	3	7	3	2	1	8
Total for Consultation (d)	35	40	39	45	35	24
Damaged (e)	14	11	11	16	9	3
Not Damaged (f)	21	269	28	29	26	21
Grand Total (a + d)	44	60	48	53	42	38
Damaged (b + e)	20	24	17	22	15	9
Not Damaged (c + f)	24	36	31	31	27	29

(1) Reporting Status for Unauthorized Computer Access

Reported number in July was **14**: 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 **24** (of **2** were also counted as reported number): Of **3** was the number actually damaged.

(3) Status of Damage

The breakdown for damage reports included intrusion with **2**, source address spoofing with **1** and masquerading with **3**.

As for the damages caused by intrusion were: backdoor program was embedded with 1 and malicious script was embedded within a webpage with 1. The cause of intrusion was that vulnerability relevant to cgi within a server was exploited (the cause for the other case has 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 3) without asking.

***Backdoor:** A trap (s) which makes it possible for an intruder to re-sneak into the computer system left in a system when the intruder previously intruded.

***cgi (Common Gateway Interface):** A mechanism to be used by a web server to send out a client a certain consequence obtained by operating a program on that web server according to the client’s request.

(4) Damage Instance

[Intrusion]

(i) Vulnerability of cgi was exploited and intruded: backdoor was located therein...

Instance	<ul style="list-style-type: none">-IDS (intrusion detection system) detected such attack seemed to be OS command injection.-Study was conducted: it was realized that the vulnerability of cgi program used on our web server was exploited and intruded then the php shell program which conducts backdoor function so called “madshell” was embedded and executed.-We decided to reconstruct the subjected server, accordingly.
----------	---

[Masquerading]

(ii) My item and pockets to be used on on-line games were stolen...

Instance	<ul style="list-style-type: none">-Upon logged in to the on-line game site where I signed up with, I was realized that the item and money possessed by my avatar were missing.-When I checked archives accordingly; it was realized that someone spoofed to be myself logged in to the site and he/she gifted my items, etc. to the other avatar without asking.-The cause has not yet been clarified.
----------	--

IV. Accepting Status of Consultation

The gross number of consultation in July was 1,708. Of the consultation relevant to “**One-click Billing Fraud**” was **657** (June: 694): this bad figure was continually maintained from the previous month. The consultation relevant to “**Hard selling of falsified anti-virus software**” was **6** (June: 6), the consultation relevant to “**Winny**” with **6** (June: 13), were also realized. (The consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” was **1** (June: 0).

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

	Feb.	Mar.	Apr.	May	Jun.	Jul.
Total	1,051	1,406	1,668	1,765	1,898	1,708
Automatic Response System	521	758	962	992	1,081	923
Telephone	472	597	651	710	777	736
e-mail	57	49	55	58	37	47
Fax, Others	1	2	0	5	3	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, winnyl19@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. Reporting Status of Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

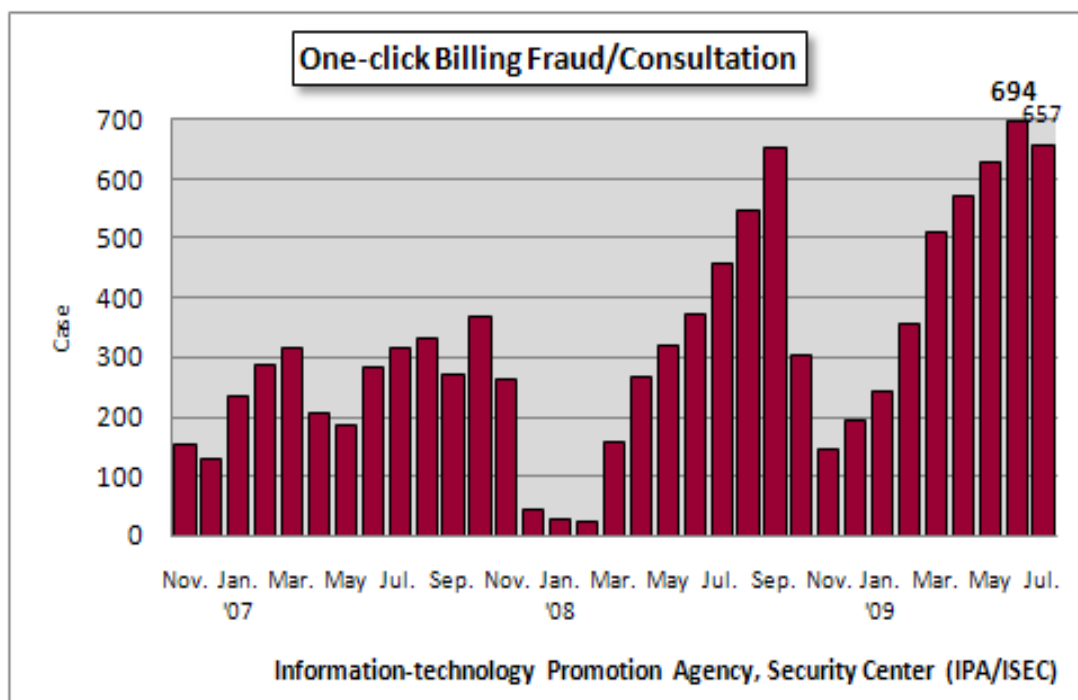


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) Can you tell me about security measures for officially publicized server and computer network...?

<p>Consultation</p>	<p>We are considering about the security measures for officially publicized server and internal (computer) network. Can you tell me what type of security measures should be done in general and how far?</p>
<p>Response</p>	<p>We cannot tell it to you easily as the security measures required are differed from respective corporations or organizations, etc. First of all, you have to analyze current security measures employed within your business and to subsequently review further suitable security measures based on the consequences obtained from the analysis. We are officially publicizing the guidelines: please also refer them for your further information.</p> <p><Reference> The Guidelines for IT Security Measures for Small and Medium Sized Businesses(IPA)(in Japanese) http://www.ipa.go.jp/security/fy20/reports/sme-guide/press.html</p>

(ii) My friend (s) is reluctant to conduct anti-virus measures...?

<p>Consultation</p>	<p>I used to suggest my friend (s) to conduct certain anti-virus measures for his/her computer. However, he/she is reluctant to do with the following reasons.</p> <ul style="list-style-type: none"> - Computer with anti-virus software behaves slower. - He/she does not like to spend more money for the computer. - He/she does not stored important data on the computer so that he/she would not lose anything even if infected. <p>Accordingly, he/she does not even attempt to install anti-virus software. How I can convince him/her.</p>
<p>Response</p>	<p>The acquaintance may become a casualty if he/she continually uses the computer infected as it is since virus (es) may automatically send spams and/or attacks the other site (s). If he/she left the computer as it is, he/she will get alerts from the provider and/or he/she may be denied to connect to the Internet one-sidedly. You can convince him/her telling that “to maintain virus-free net society, it is necessary that every user has to aware security and to conduct adequate (security) measures on an individual basis”. Here in IPA, we provide variety of information that can be helpful to conduct effective security measures.</p> <p><Reference> Brochures for Variety Security Measures(IPA) (in Japanese) http://www.ipa.go.jp/security/antivirus/shiori.html</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in July was **148,935** for the 10 monitoring points and the gross number of source* was **57,687**. That is, the number of access was **480** from **186** 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.

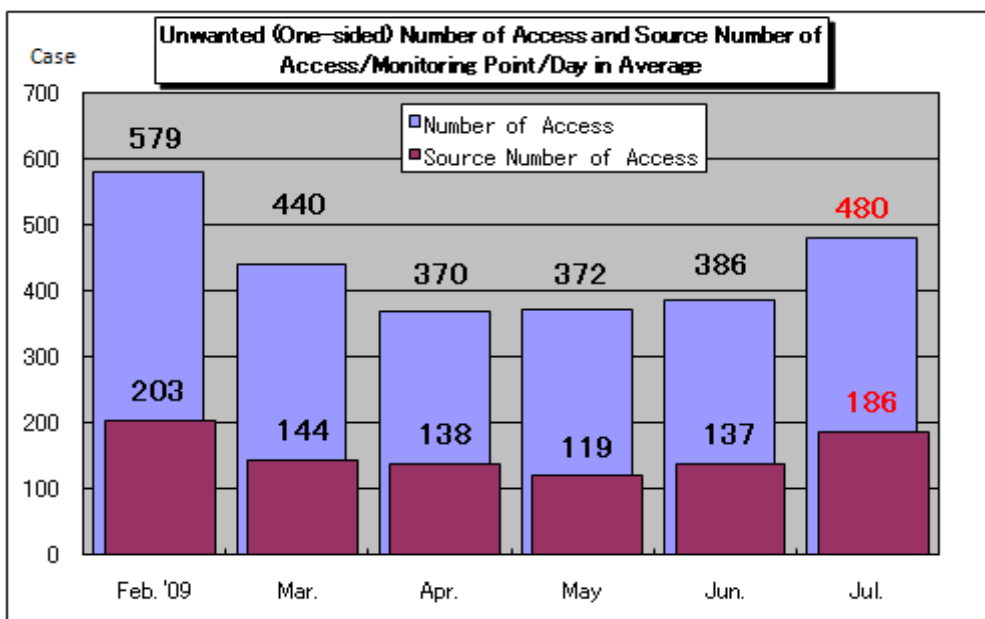


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

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

The Chart 5-2 shows the comparison of number of access classified by destination (by port) for June and July. In July, the access to the port 445/tcp was further increased from the one in June. The cause of access increase in June was that the number of access from overseas was increased: this scenario was still continued in July: thereby the access increased to the port 445/tcp (See the Chart 5-3). The cause for that access increase has not yet been clarified: as with June, the number of access from overseas further increased, but none of number of access from specific source was increased.

In July, access to several ports such as 22862/tcp, 12370/udp, 7259/udp, etc. were monitored: they were the ports that none of access was monitored in June. The cause for their accesses to these ports was unknown; they were monitored at single specific monitoring point respectively.

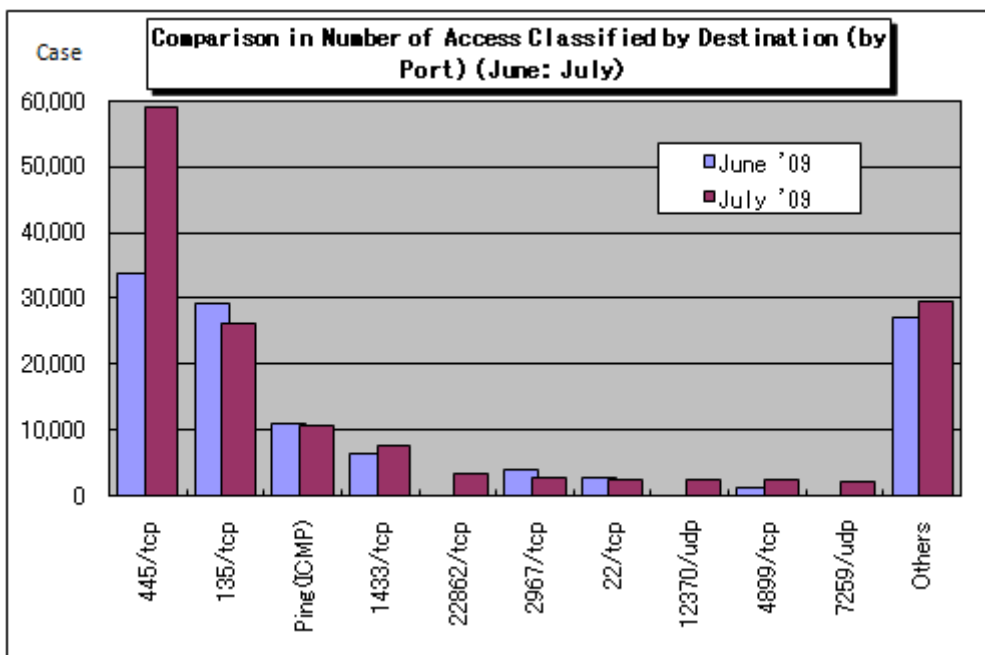


Chart 5-2: Comparison in Number of Access Classified by Destination (by Port) (June: July)

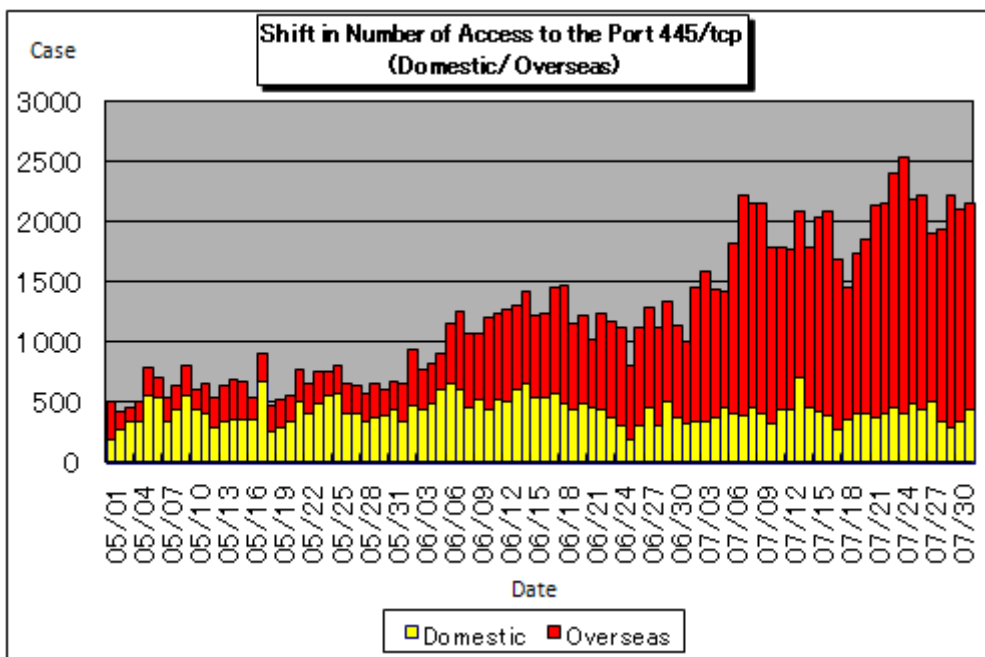


Chart 5-3: Shift in Number of Access to the Port 445/tcp (Domestic/Overseas)

(1) Access to the Port 4899/tcp

In the middle of July, there is a period for which access to the port 4899/tcp was increased, but temporarily. This was the cause that the access from one of Korean sources and accesses from several sources from South America such as Argentina, Venezuela, Columbia, etc. were increased (See the Chart 5-4).

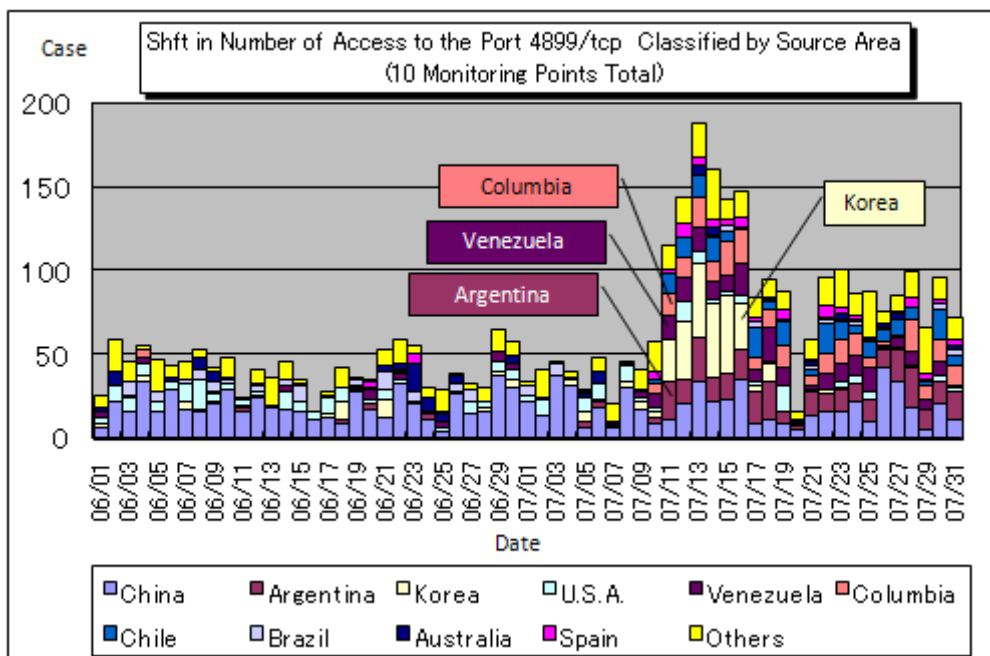


Chart 5-4: Shift in Number of Access to the Port 4899/tcp Classified by Source Area (10 Monitoring Points Total)

The access increase to the port 4899/tcp from South America was also monitored by the other organizations where conduct fixed-point observation: in another words, similar event may have been caused over a quite wide area.

The port 4899/tcp was known as the port used by Radmin, the remote control software by Famatech.

Accordingly, those Radmin users should check if your computer is not allowing access to the port 4899/tcp from unauthorized source (s). Be sure to restrict access to the port (squeezing of IP address to be allowed for access) and/or to harden access authentication.

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/200907/documents/TALOT2-0907.pdf>

Summary Reporting Status for Computer Virus/Unauthorized Computer Access for July
<http://www.ipa.go.jp/security/english/virus/press/200907/documents/summary0907.pdf>

Attachment_1 Computer Virus Incident Report
<http://www.ipa.go.jp/security/english/virus/press/200907/documents/virus0907.pdf>

Attachment_2 Unauthorized Computer Access Incident Report
<http://www.ipa.go.jp/security/english/virus/press/200907/documents/crack0907.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