

## **Computer Virus/Unauthorized Computer Access Incident Report**

*- November 2009 -*

### **<In Response to the Drastic Increase of the “One-click Billing Fraud” relevant Consultation, We Emergently Publicized the Countermeasures Information on Our Web Pages>**

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

#### **I. Reminder for the Month**

**Ensuring Security on the Internet is your own responsibility!! It is you who'd clicked “Yes”  
- Be sure to realize the traps relevant to One-click billing fraud -**

The consultation number relevant to “One-click billing fraud” filed with IPA having been exceeded 600 cases/month over the continuum of 7 months – In November, it eventually marked 903, the worst figure ever (See the Chart 1-1). There were 2 major causes: the one is the number of such website which newly conducts “One-click billing fraud” was increased and the other one is such methodology which induces users to such website is getting further sophisticated.

Accordingly, the fundamental (i.e., the best) countermeasures against such fraud is to know their methodology (ies). Upon viewing websites, be sure to read the “notes (hereinafter we referred it as terms of service)” appeared on the screen carefully to prevent involving yourself with unwanted troubles: i.e., if you do not totally intend to sign-up, be sure NOT to click “Yes” at the confirmation/verification window. On this occasion, be sure to understand how to get recovered in case you would get troubled.

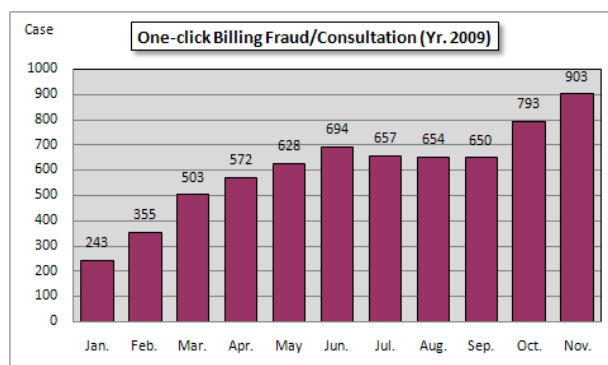
For further details, please refer to: <http://www.ipa.go.jp/security/topics/alert20080909.html> (in Japanese)

#### **(1) Current Status of “One-click Billing Fraud”**

“One-click billing fraud” is the one of methodologies which exploits user’s psychology who’d clicked “Yes” over and over to go forward to view adult movies with free of charge: in this methodology, the user may be signed up with the site while he/she does not know by the website manager to bill the user lately. Of some methodologies, there involve viruses which infect user’s computer to bill the user over and over to drive up the user psychologically.

Here in IPA, we filed quite a few consultations from users regardless of their age or their gender, etc. We recognized that not only adults, but children and elder people are induced to fraudulent sites as this fraud is now deployed to every sort of categories such as anime site, game site, etc.

In November, we identified a new hoax site which deceives users to provide estimated information about the winner horse (s) in certain horse race (s). Accordingly, we are afraid that the similar hoax methodology (ies) will be spread out in different categories other than adult sites.

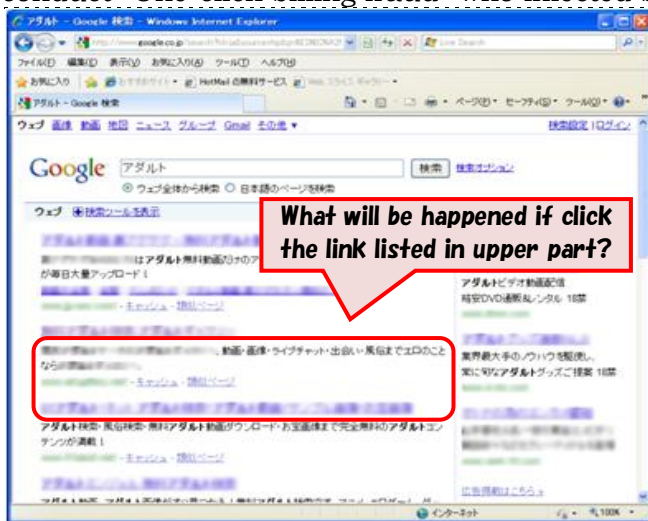


**Chart 1-1: One-click Billing Fraud/Consultation**

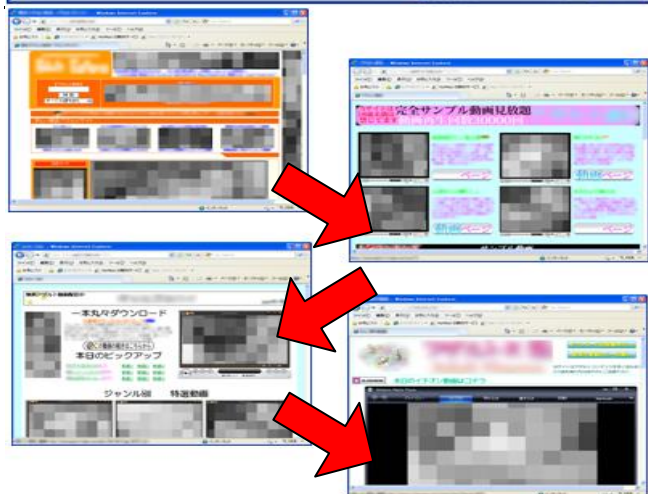
As for the latest “One-click billing fraud”, it is getting further difficult to identify which part (s) is actually conflicts with the law so that it is hard to determine that “they are absolutely illicit.” Rather, it is possible that the user’s responsibility who’d easily clicked “Yes” will lead social criticism.

## (2) Current “One-click Billing Fraud” Methodology

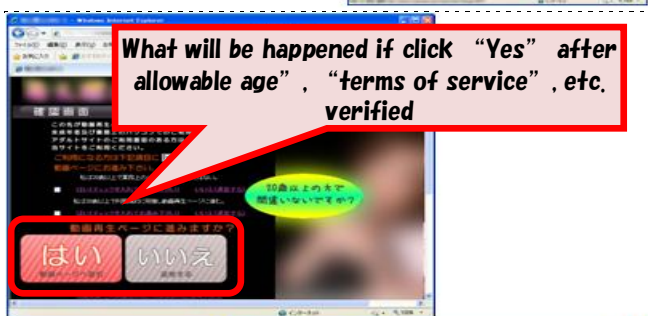
Follows, we will show you a series of processes that a user induced to the website which conduct “One-click billing fraud” who infected by virus.



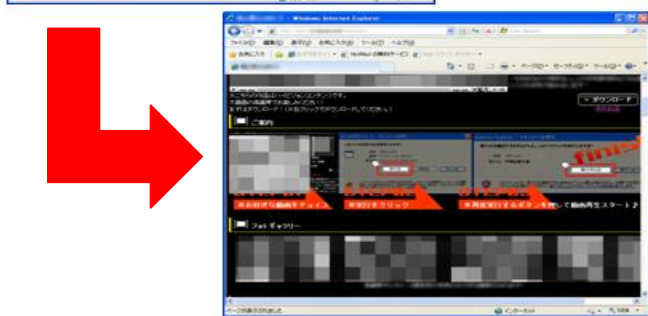
[a] Let's start to search the site (s) with the keyword such as “adult”, “free”, “movie”, etc. Of the results appeared by the search engine, we attempted to click the link for the site listed at the upper portion of the results.



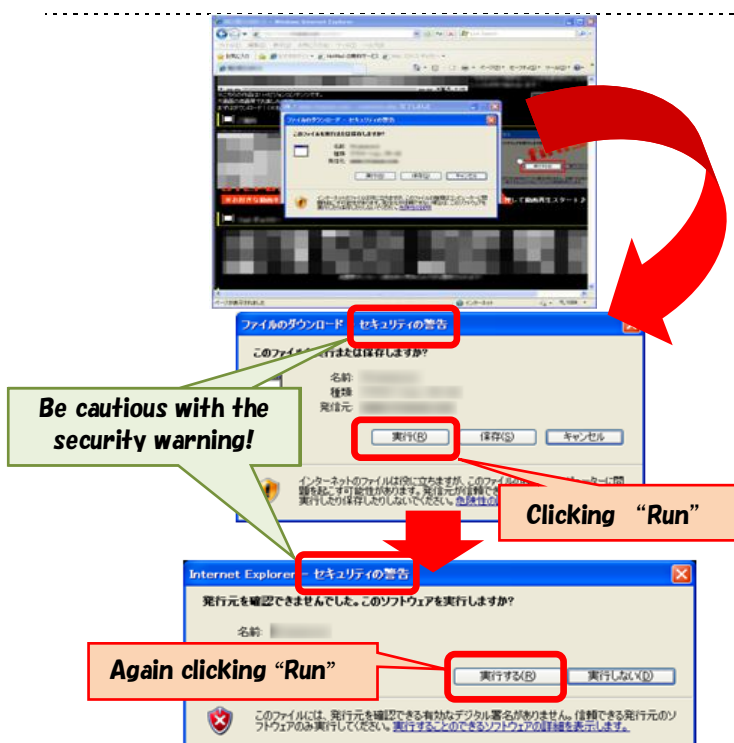
[b] Let's click the image to attempt to replay free movie at the site jumped from the search engine. What will be happened in the next? As you can see, we are being induced to the website which conducts “One-click Billing Fraud” via intermediate (malicious) websites. For your further information, there isn't a word which refers “free” in the website we'd eventually arrived. In this way, users will be tactfully induced from “hoax” free site to “charged” site. In addition, users feel pressed as they pass through several intermediate websites so that they may be distracted eventually.



[c] There are several check boxes to have users verify “if they are in allowable age”, “whether they can agree with the terms of service or not”, “whether the computer now the user in use is for office or not”, etc. Upon clicking “Yes” for all items, then, the user will be sent to the page in where movies will be replayed (in case you do not click “Yes” to all items, you cannot go forward). In this instance, the “terms of service” is (intentionally?) designed to locate under the “Yes” button. To read the contents, users need to scroll it down, accordingly.



In the page you'd eventually arrived, there may be described some procedures how to play movies: in this instance, the site will instruct the user to click “Run” button if the alert shown in the [d] is appeared.



[d] When you attempt to replay movies, the small window so called “Security Alert” is appeared. As stated in the [c] above, we attempt to click the “Run” button. Well, the same window so called “Security Alert” is appeared again. What will be happened if we click the “Run” button again?

- \* Generally, such operation will not be required if you simply replay (legitimate) movies. Please be noted that the “Security Alert” will only be appeared if some sort of program (usually a malicious program) is downloaded in your computer. As you already learned that the “Security Alert” means that you are in hazardous state so that you must stop to further click to go forward.



[e] Via a series of operations described in the [d] above, the virus which will inform you that “your sign-up is completed” will be embedded.

In the event, each time, upon booting-up the computer, the screen which tells you that “your sign-up is completed” will be automatically appeared. In addition, this screen will be shown on and off with certain intervals while the computer is in use.

For your further security, we are introducing several methodologies relevant fraud inclusive of the instance above in the following URL. Please visit here for your further reference.

<Reference>

IPA – Security Alert relevant to One-click Billing Fraud (as of December 3, 2009) (in Japanese) <http://www.ipa.go.jp/security/topics/alert20080909.html>

(3) Preventive Measures

Most of all damages relevant to “One-click Billing Fraud” occur at adult sites. To prevent yourself get involved from such damage (s), be sure to check the “terms of service” carefully and do not make hast to view adult movies.

(a) For PC users – do not click “Yes” buttons easily at the verification/confirmation screen  
 If you can see “Yes” and “No” buttons attempting to verify “if you are in allowable age to view the site” or it urges you to agree the terms of service, be sure to ask yourself “why I am going to click “Yes” here?” Most of all websites which conduct “One-click billing fraud” locate “Yes” buttons

in the proximity of their terms of service. It is probably a charged-site if certain amount is clearly stated in the terms of service. Accordingly, the activity to go forward by clicking “Yes” buttons over and over means that you are going to agree with the contents of the terms of service. It is hard to determine whether such a website is legitimate or illegal and your responsibility who’d easily clicked “Yes” buttons may also be questioned. Be sure to check the contents what they say in the terms of service and, never, ever click “Yes” if you do not INTEND to sign-up with the site. Be sure to halt yourself and close the page immediately.

(b) For home users with juveniles – employs malicious site blocking software/service

There reported number of cases that juveniles in elementary/junior high school also gets involved with the damage relevant to “One-click billing fraud”. We encourage such family who shares their home computer with juveniles to install such software which blocks malicious sites (the software is also referred as web filtering software/URL filtering software). With malicious site blocking software, you can block your kids viewing improper websites such as adult site, illicit drug-information, etc. Since any of adult sites that trap users “One-click billing fraud” can be blocked so that the damages can also be prevented. For your information, some providers may provide such service that can block malicious sites. In case you are not able to configure the said blocking software by yourself, we will recommend you to consult the provider you are signing-up with to employ their service.

#### **(4) Recovery Methods**

In case your computer is infected by virus and billing statement is automatically appeared over and over, be sure to conduct “system recovery” which specifically described below. Even though the symptom is not remedied or the “system recovery” is somewhat failed, it is possible to perfectly remove the virus by initializing your computer.

(a) Recovery by “System Recovery”

Windows XP/Vista/7 furnish “System Recovery” function that can restore back your computer to the previous state based on the system information the computer automatically stored in case your computer unstably behaves and/or is unable to use. Please refer to the following URL when you conduct “System Recovery”. However, if you installed application software, updated information, etc. you’d done before the date you’ve specified from now will be vanished so that you need to do that again after you are successfully recovered.

<Reference>

IPA – Windows “System Recovery” (in Japanese)

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

(b) Initialization

This terminology refers to restore back your computer to the initial state when the computer is shipped out from its manufacturer. As for actual work procedure, please refer/follow to the “how to restore back the computer initially purchased” column in your instruction manual. We encourage you to back up important data to outside memory media such as USB memory, CD-R, or outside HDD, etc. before you start to work.

For your information, to perfectly RESTORE Windows 2000, it is necessary to modify its registry. In case the registry is not properly modified (i.e., if you failed to modify the registry), it is highly probable that your computer cannot be able to boot-up. Accordingly, IPA rather recommends you to INITIALIZE your computer in case you have damages while using Windows 2000.

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

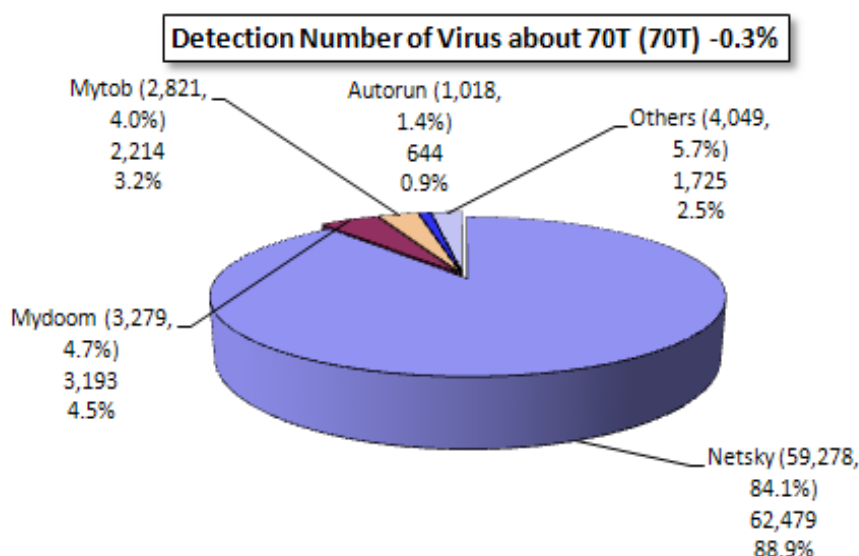
**(1) Reporting Status of Virus**

The detection number of virus<sup>(\*)</sup> in November was about 70T: shifted with same level with about 70T in October. In addition, the reported number of virus<sup>(\*)</sup> in November was 1,140: 5.8% decreased from 1,210 in October.

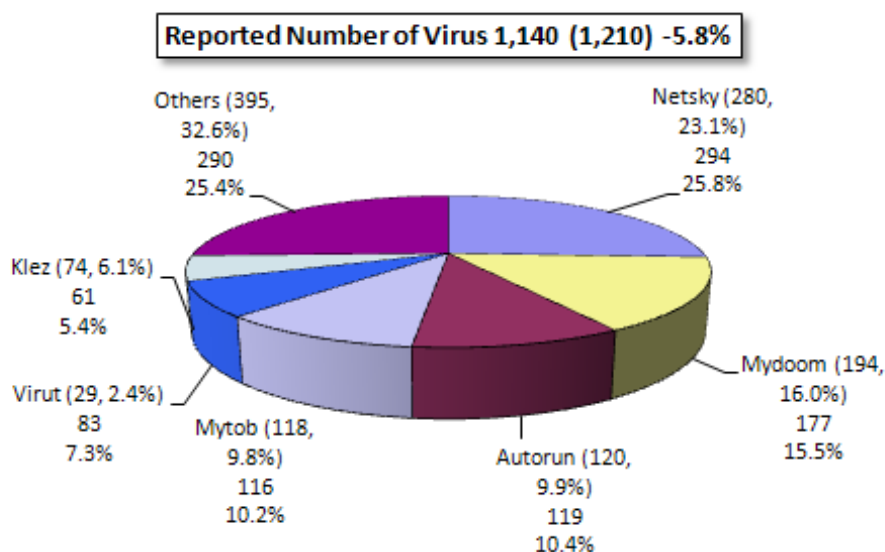
(\*) Detection number: Reported virus counts (cumulative) found by a filer.

(\*) 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 November, the reported number was 1,140 and the aggregated virus count was about 70T.

The worst detection number was W32/Netsky with about 62T: W32/Mydoom with about 3.2T and W32/Mytob with about 2.2T followed.



**Chart 2-1: Detection Number of Virus**



**Chart 2-2: Reported Number of Virus**

**(2) Detection Status of the Falsified Program**

The detection number of “Falsified Security Software” type of virus (FAKEAV) which drastically increased in September 2009 got declining thereafter and returned to the previous level in November as it was (See the Chart 2-3).

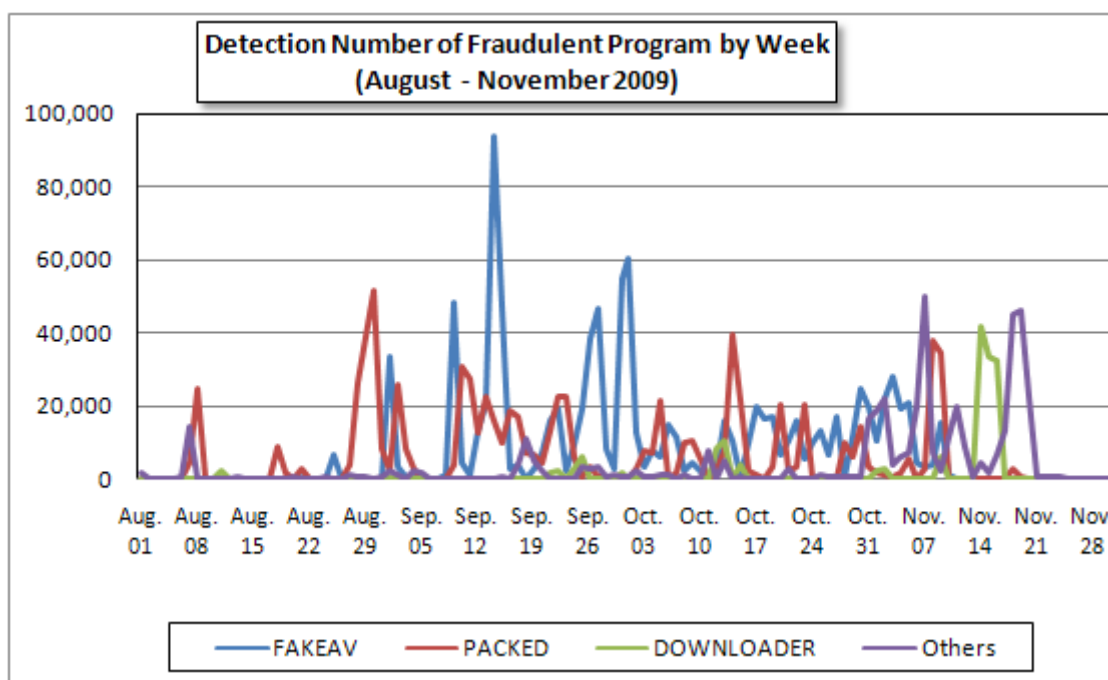
Such falsified program is likely distributed as attachment file to e-mail; as the Chart 2-3 shows, they moved artificially as they drastically increased at specific period, etc. The one can be assumed is that they may have been distributed via bot-infected mail, etc. We cannot foresee when they will increase, accordingly; we have to pay attention to it continuously.

In the Cyber Clean Center (CCC), they provide effective anti-bot measures as well as its removable tool with free of charge. Be sure NOT to be a victimizer by distributing bot-infected mail while you do not know. To that end, be sure to conduct certain anti-bot measures such as check with or without bot regularly, try not to install malicious program in your computer, etc.

**<Reference>**

“The Knowledge How to Prevent from Virus Infection” (Cyber Clean Center) (in Japanese)

<https://www.ccc.go.jp/knowledge/>



**Chart 2-3: Fraudulent Program/Detection Number/Week**

**III. Reporting Status of Unauthorized Computer Access (includes Consultations) –**  
*Please refer to the Attachment 2 for further details –*

**Chart 3-1: Reported Number for unauthorized computer access and the status of consultation**

	June	July	Aug.	Sep.	Oct.	Nov.
<b>Total for Reported (a)</b>	<b>7</b>	<b>14</b>	<b>20</b>	<b>11</b>	<b>21</b>	<b>11</b>
Damaged (b)	6	6	12	8	14	6
Not Damaged (c)	1	8	8	3	7	5
<b>Total for Consultation (d)</b>	<b>35</b>	<b>24</b>	<b>39</b>	<b>44</b>	<b>34</b>	<b>34</b>
Damaged (e)	9	3	17	13	11	14
Not Damaged (f)	26	21	22	31	23	20
<b>Grand Total (a + d)</b>	<b>42</b>	<b>38</b>	<b>59</b>	<b>55</b>	<b>55</b>	<b>45</b>
Damaged (b + e)	15	9	29	21	25	20
Not Damaged (c + f)	27	29	30	34	30	25

**(1) Reporting Status for Unauthorized Computer Access**

Reported number in November was **11**: 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 **34** (of **5** were also counted as reported number): Of **14** was the number actually damaged.

**(3) Status of Damage**

The breakdown for the damage reports were **intrusion** with **1** and **masquerading** with **5**. The damage for the “Intrusion” included: unauthorized computer program was located to the web server to attack to the other site was 1. The “Intrusion” was caused by the Password cracking attack to the port used by SSH. As for the “masquerading”, someone masqueraded to be the legitimate user for the online services logged in and used the services fraudulently was 5 (online game site with 4, second-hand car trading site with 1).

\* SSH (Secure Shell): One of the protocols which enables communication with the computer remotely located via a network.

\* Password Cracking Attack: One of fraudulent activities which analyze/parse someone’s password. Brute-force attack (or Exhaustive search attack) and Dictionary attack are well-known. There exist cracking-oriented programs as well.

(4) Damage Instance

**[Intrusion]**

(i) The web server used by SSH was attacked and intruded ...

Instance	<ul style="list-style-type: none"> <li>-“Our web server is being accessed fraudulently by the web server in your campus” so communicated from outside of the campus.</li> <li>-Study was conducted: then, it was realized that the port to be used by SSH for the web server in our campus was conducted by Password cracking attack: in the event, the web server was intruded and its administrator privilege was hijacked.</li> <li>-The cause was the password for the root - easily assumable password was configured. In addition, users could SSH log-in at the root – it was another cause that the damage was worsened.</li> </ul>
----------	---

(ii) My account was hijacked at one of the online game sites ...

Instance	<ul style="list-style-type: none"> <li>-I am using charged online game site. Since I developed unauthorized access attempt on November 27; I changed my password on the very next day, the November 28. I configured the new password with 12 characters inclusive of alphabets and numbers.</li> <li>-On November 29, I attempted to log in, but I was unable to get in: my computer prompted me that my password is differed.</li> <li>-In this game site, user is able to see my avatar without entering my password. I was realized that someone masquerading to be me was hijacked my account as the avatar was apparently differed with the one I previously configured.</li> <li>-I anyway informed the facts to the online game site manager; however, I cannot hear from him/her as of now.</li> </ul>
----------	---

#### IV. Accepting Status of Consultation

The gross number of consultation in November was 2,315. It became the worst. The consultation relevant to **“One-click Billing Fraud”** was **903** (October: 793): The bad figure was again worsened drastically (See the Chart 4-1). The others included the consultation relevant to **“Hard selling of falsified anti-virus software”** with **6** (October: 6), the consultation relevant to **“Winny”** with **0** (October: 3), the consultation relevant to **“the suspicious mail sent to specific organization to collect specific information/data”** with **0** (October: 0), etc.

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

	June	July	August	Sept.	Oct.	Nov.
<b>Total</b>	<b>1,898</b>	<b>1,708</b>	<b>1,792</b>	<b>1,653</b>	<b>2,049</b>	<b>2,315</b>
Automatic Response System	1,081	923	1,015	915	1,157	1,340
Telephone	777	736	702	676	843	918
e-mail	37	47	68	60	45	53
Fax, Others	3	2	7	2	4	4

\*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](mailto:virus@ipa.go.jp) for virus issues, [crack@ipa.go.jp](mailto:crack@ipa.go.jp) for crack issues, [winny119@ipa.go.jp](mailto:winny119@ipa.go.jp) for emergent consultation relevant to Winny, [fushin110@ipa.go.jp](mailto:fushin110@ipa.go.jp) for suspicious mail handling and [isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp) for other security relevant issues.

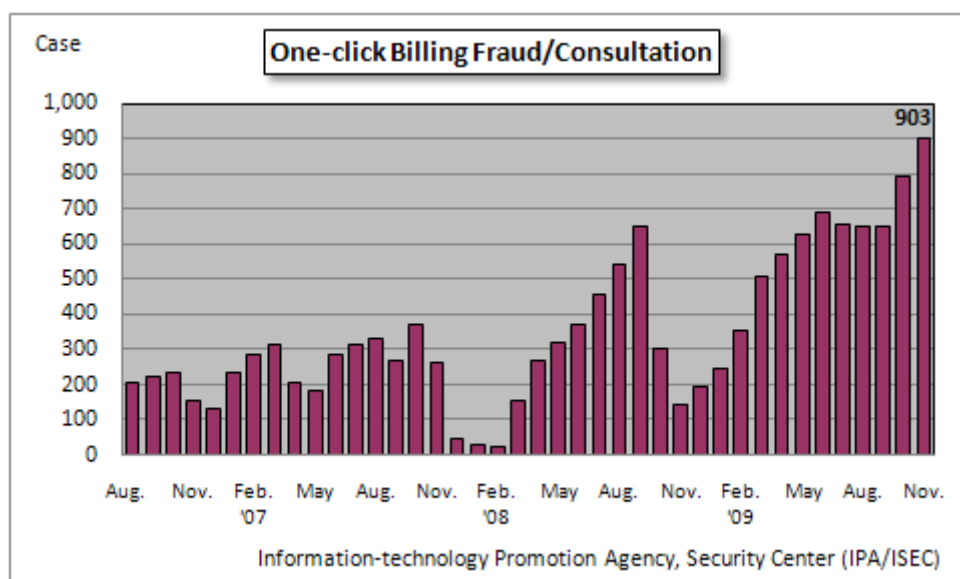
Tel.: +81-3-5978-7509 (24-hour automatic response; in person consultation by an IPA Security Center personnel is available from Mon. – Fri., 10:00 – 12:00, 13:30 – 17:00.)

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 <sup>(d)</sup> 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) I was billed as I went forward by clicking “Yes” to browse movies with YouTube ...?

<p><b>Consultation</b></p>	<p>I was in the YouTube (a movie posting site): When I clicked the link next to the comments of the original poster, I was eventually sent to an adult site. I know that the YouTube is the free movie site so that I believed that the sites to where I jumped were also free: accordingly, I clicked sample images over and over to view some adult movies. In the event, I was signed-up with the site while I did not know and billed ¥50,000 (about \$5,000.00). Though I rebooted my computer, the billing statement screen appears on and off several minutes of intervals.</p> <p><b>(Other than this consultation, we filed similar damage reports relevant to YouTube more than 20 cases in November.)</b></p>
<p><b>Response</b></p>	<p>We’d identified such movies that can trap PC users induce to “One-click billing fraud” site (s) which posted in YouTube. Even you clicked from one of renowned sites, there is none of assurance that the site you jumped to is also secured. The most of all site (s) you jumped to, they clearly state that they are charged sites in the proximity of “Yes” buttons. Accordingly, the fundamental (i.e., the best) countermeasures to prevent from such malicious sites, it is utmost important to read the terms of service site by site or even screen by screen. Be sure not to be tempted and make sound decision!</p> <p><b>&lt;Reference&gt;</b>          IPA – “[Information calling for attention] Consultation relevant to one-click billing fraud is significantly increased!” (in Japanese)  <a href="http://www.ipa.go.jp/security/topics/alert20080909.html">http://www.ipa.go.jp/security/topics/alert20080909.html</a></p>

(ii) When I browsed adult sites with the common use computer in my office, the billing statement was unable to be disappeared ...?

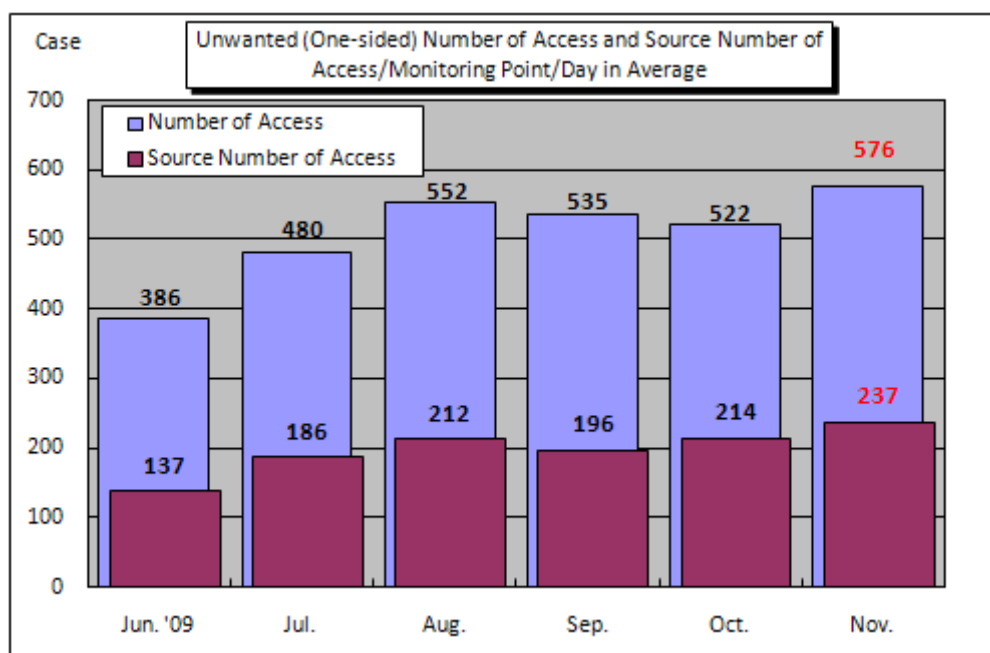
<p><b>Consultation</b></p>	<p>I sneaked to browse an adult site with the common use computer in my office. I believed that the site was free: when I was realized, there appeared the billing statement. Though I rebooted the computer over and over, the billing statement appeared with several minutes of intervals. I consulted with IPA – the personnel explained me that I was trapped to “One-click billing fraud” and the common use computer was infected to the virus which shows the billing statement so that I totally removed the virus. With my sincere apology, I explained my story to alert to my colleagues. However, about 2 weeks later, again, billing statement is getting appeared. It differs from the previous one. I have no idea who did it.</p>
<p><b>Response</b></p>	<p>You and your colleagues do not understand the ground so that your bitter experience is not completely leveraged. The root problem relevant to “One-click billing fraud” is to click “Yes” buttons to agree with the terms of service though you do not intend to sign up with the site. Adult sites or viruses are not the root problem at all. It is always your own responsibility who’d clicked “Yes”. Such excuse that “even I clicked “Yes”, I did not want to sign up” is not always valid. Be sure to read the terms of service carefully what it says and behave with due diligence; then you will be able to prevent unwanted troubles before it happens.</p> <p><b>&lt;Reference&gt;</b>          IPA – “[Information calling for attention] Consultation relevant to one-click billing fraud is significantly increased!”  <a href="http://www.ipa.go.jp/security/topics/alert20080909.html">http://www.ipa.go.jp/security/topics/alert20080909.html</a></p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in November was **172,802** for the 10 monitoring points and the gross number of source\* was **71,136**. That is, the number of access was **576** from **237** source addresses/monitoring point/day.

\*Gross number of source: the gross number of the source accessed to 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 in average from June to November 2009. Both the unwanted (one-sided) number of accesses were increased from the ones marked in October.

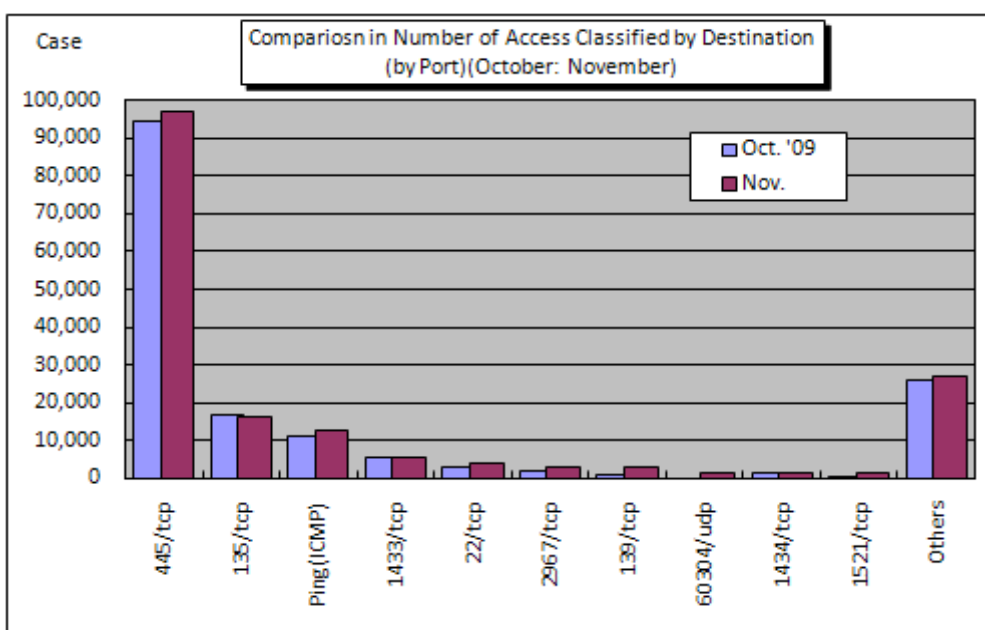
The Chart 5-2 shows the comparison in number of access by destination (by port) in October and November. In November, the number of access was entirely increased with several reasons: The one was the number of access to the port 60304/udp was frequently monitored (in October none of such access was monitored). The other one was the number of access to the several ports such as 2967/tcp, 139/tcp, 1521/tcp, etc. were increased.

The access to the port 60304/udp was monitored only in couple of days in the last part of November and the source was only from Australia. We cannot identify their purpose (s) of access. In addition, the number of access to the port 1521/tcp had proportionally increased the most compared with the one in October. The port 1521/tcp is the default port used by Oracle database. In TALOT2, the access increase to this port having been monitored on and around the first part of July in 2009 and the number of access was subtly increased from the last part of October as well (See the Chart 5-3). This can be monitored in several organizations who also conduct the Internet monitoring activities. We identified the site in China which distribute such tool that can scan the port 1521/tcp in the first part of July: since the access

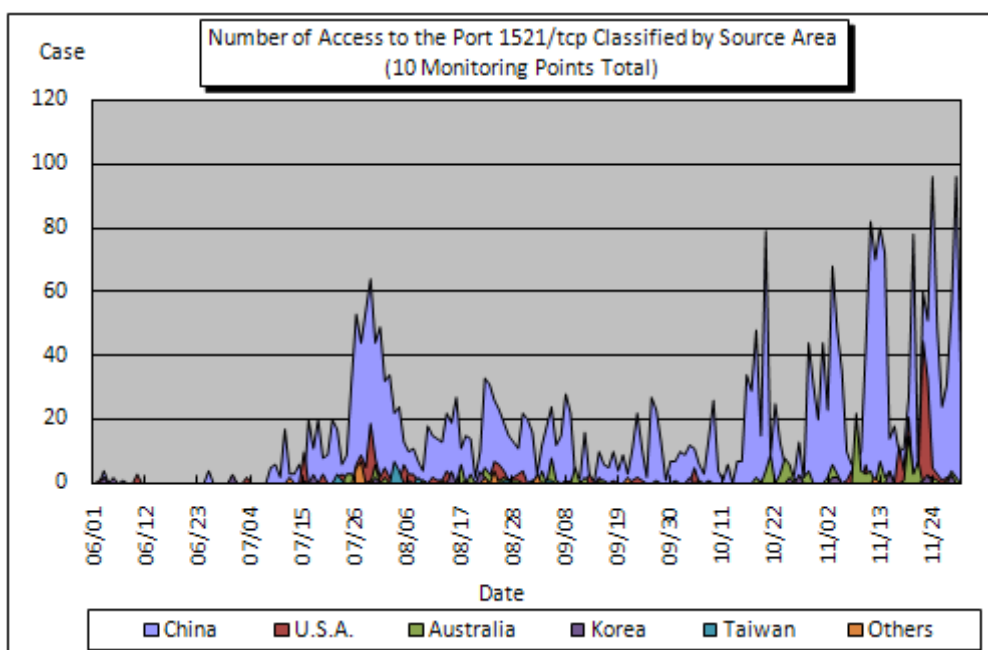
increase to this port was initially monitored on and around the first part of July; we parsed that there may have been continually accessed to the port to probe vulnerable Oracle database by using this tool.

To prevent from such access increase, following countermeasures will be of help.

- Restricting access from outside/restricting connectable IP address by firewall
- The default port number assigned for Oracle database changes to different port number
- Reconfigure the user's password for the Oracle database to the one hardly assumable
- Resolve vulnerabilities in OSs and the other application software



**Chart 5-2: Number of Access Classified by Destination (by Port) (October: November)**



**Chart 5-3: Number of Access to the Port 1521/tcp Classified by Source Area (10 Monitoring Points Total)**

**<Reference>**

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/200911/documents/TALOT2-0911.pdf>

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

<http://www.ipa.go.jp/security/english/virus/press/200911/documents/summary0911.pdf>

Attachment\_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200911/documents/virus0911.pdf>

Attachment\_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/200911/documents/crack0911.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/>

@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](mailto:isec-info@ipa.go.jp)