

Computer Virus/Unauthorized Computer Access
Incident Report – September 2009

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

I. Reminder for the Month

“Your Avatar in Online Games are being Targeted!”
– My game items are all vanished, suddenly?! –

Currently, the consultations and the reports of the damages relevant to online games are rushed to IPA. The major damages are the cause by the account hacking in general sense: the user IDs and passwords necessary for online games were fraudulently used by someone and the items (such as arms, coins, etc. to be used by the avatar in games) to be used by his/her avatar in the games were stolen.

The one reason to make it increase such damage is that the items in online games are actually tradable with real money. They are priced vary, but the most of them are priced very expensively so that they are easily targeted by criminals for money.

Accordingly, online users should recognize the risk that “you are always targeted” and take necessary self-protective measures to prevent from such damages.

(1) Damage Instances by Online Games

Online games are defined to be the games that are subscribed by unspecified majority users via the Internet. The total number of consultation/reports relevant to online games rushed to IPA from January to September 2009 is 31. Of the more than the half (i.e., 16) were caused from July to September and the damages are tended to increase.

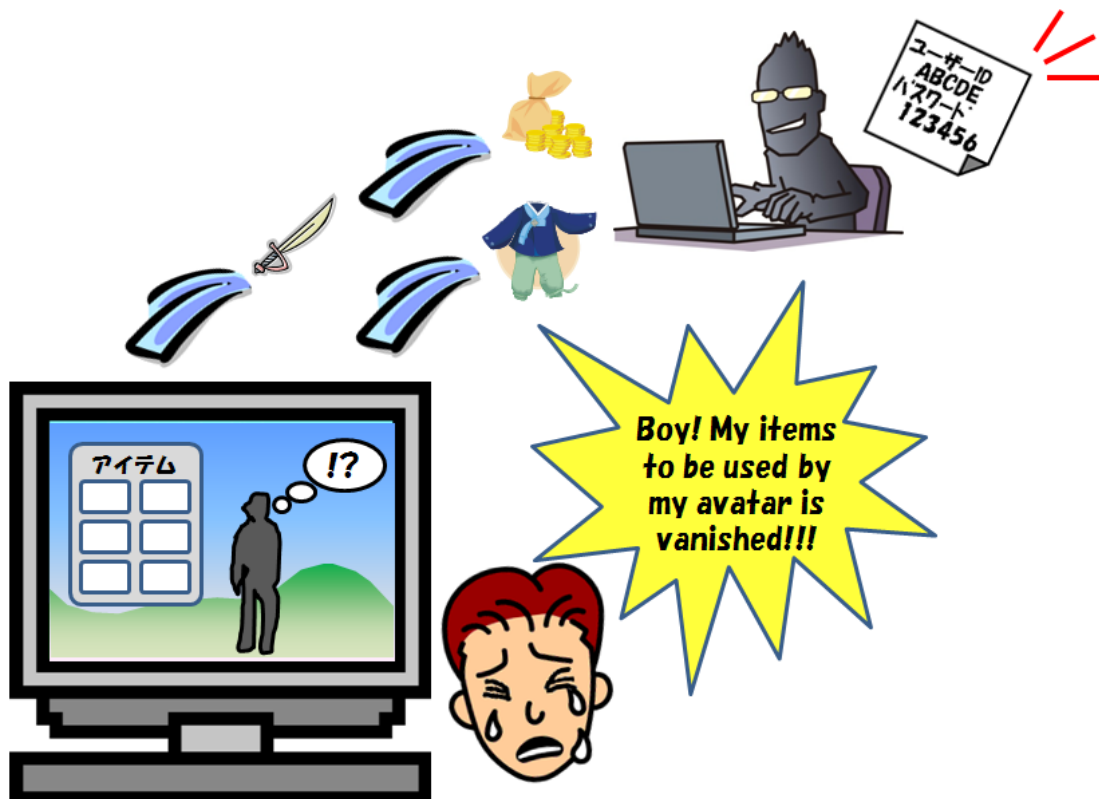


Chart 1: Items for Online Games were Stolen by Account Hacking

Follows are the specific damage instances filed by concerned windows in IPA.

Instance 1: <Items to be used by the avatar in game (s) is stolen>

While chatting with the user met while playing game (s), This person was insistently urged to download/install the tool by him/her saying that “the tool is convenient for the games”. However, the tool was actually the virus which steals user IDs and passwords for games. When I logged in to the games subsequent days, my items to be used by my avatar in the games were stolen.

Instance 2: <ID and password for games was fraudulently inquired>

While a user was playing game (s), someone who identifying him/herself as the “site manager” requested me to chat: the user responded to it as the user thought that the “site manager” was patrolling the site and told him/her this person’s ID and password as the “site manager” inquired that he/she needed it for just verification. The person who identified him/herself as the “site manager” was actually a malicious user: when realized it, all the items to be used by the user’s avatar in games were stolen.

In the instances above mentioned, the major damage for account hacking would cause leakage of user IDs and passwords. Follows, we will show you the methods that may cause the leakage of user IDs and passwords.

(2) The Methods

The method for the instance 1 above is as follow.

Method 1: <Infection by the virus which steals user IDs and passwords>

Users may have infected by virus via following careless activities: opening of appended file to e-mail in which some virus is embedded; accessing of website (s) in where some virus is trapped; connecting of outside memory media in which some virus is already infected such as USB memory, etc. to your computer. In addition, some virus may have been trapped to some of game capturing site (s).

The method for the instance 2 above is as follow.

Method 2: <Password inquired by social engineering and/or by the direct trading with malicious user>

With the snow jobs such as “I will gift you my item (s)”, “I will buy your items with high price”, etc., (legitimate) users may tell malicious user his/her ID and/or password with ease. The malicious user may identify him/herself as the “game site manager” or the “site manager”, etc.

(3) The Countermeasures for Online Game Users

To prevent relevant damages, be sure to conduct following countermeasures.

(i) Preventive measures

The preventive measures against the method 1 above are the same with the general anti-virus measures described below.

- Resolving of vulnerability (ies) in OSs and applications.
- Installing of anti-virus software and its signatures are always up to dated.
- Do not connect outside memory media such as USB memory, etc. which you are not managing to your computer or do not insert your outside memory media such as USB memory, etc. to the computer you are not managing.

<Reference>

“Are you properly aware what is vulnerability?” (IPA) (in Japanese)

http://www.ipa.go.jp/security/vuln/vuln_contents/

“The tips how to prevent infection by virus” (IPA) (in Japanese)

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

To prevent from the damages relevant to the method 2 above, be sure to be cautious with the following items daily.

- Do not tell your ID and password to anyone (incl. your friends): do not tell them even your family members and/or your relatives.
- Be sure to ignore sweet deals: as with the same in the real world, there is trap (s) in any of sweet deals in the virtual world as well.
- Be cautious with the leading questions between chats in games: the other side of user (malicious user) attempts to inquire your ID and password with number of sophisticated methods. If you respond to his/her inquiries directly, you may be give him/her some hints (key words) the malicious user can assume your ID and password from. When you create your password, be sure to use symbols if available with the upper case letters, lower case letters and numbers to make it harder to assume it by the malicious user.

<Reference>

“Be sure to Double-check your Password!” (Reminder for September 2008)

http://www.ipa.go.jp/security/english/virus/press/200809/E_PR200809.html

- Be cautious if inquired your ID and password: it is possible that a malicious user inquires your ID and password by masquerading to be as the “game site manager”. When you inquired your ID and password from someone who you cannot determine if you can trust or not, be sure to check it with the game site manager directly.

Other than those above mentioned, your ID and password may be deviated while you do not know when you are playing games with the computer you are not managing and the computer had been infected by virus. Accordingly, we do not encourage you to use those computers you are not managing. For your further information, it is the effective self-preventive measures to choose the game site (s) in where further effective security measures (i.e., two factors authentication method, etc.) is employed.

- * The authentication method by 2 (two) factors: along with your password, the method which combining one-time password is widely used in online banking is the one of examples.

(ii) Post Countermeasures

The major cause for account hacking is the leakage of user IDs and passwords. Accordingly, be sure to immediately change your password if realized that your items were stolen. In addition, be sure to check with or without virus, the one of damage causes for account hacking: if infected, be sure to remove them. Resolving of vulnerability (ies) in the OSs and applications in your computer is also important. And, never fail to report relevant damages to IPA: we are publicizing variety of preventive measures, countermeasures, useful information to the user’s society along with parsing the damages.

<Reference>

“Measures Against Computer Viruses and Unauthorized Computer Accesses” (IPA)

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

(Tel.: 03-5978-7509)

If you damaged over and over again even you conducted the measures above mentioned, there may be the faults at the game site manager side. In that case, be sure to check with or without the countermeasures against relevant damage (s) being publicized by the game site manager side: if publicized, be sure to follow to their instructions.

If not, the guidelines which describing their policies upon using online games may be available online, be sure to check/refer the general countermeasures when get damaged. In case neither countermeasures nor the guidelines are provided, be sure to inquire to the game site manager directly.

<Reference>

“Online Game Guidelines” (Japan Online Game Forum) (in Japanese)

<http://onlinegameforum.org/guideline090903.pdf>

As for the compensation for the damage (returning the stolen items back, etc.) should be handled by respective game site manager (s) individually you are signing up with. For your further information, you are to report the damage to the police, be sure to call/consult with the police officer near your area for subsequent responses.

In case you are not treated sufficiently/properly by the game site manager, we encourage you to consult with the National Consumer Affairs Centers of Japan near your area.

<Reference>

National Consumer Affairs Center of Japan (NCAC)

http://www.kokusen.go.jp/ncac_index_e.html

The general damage reports windows for online games are as follows.

<Reference>

“Consultation for the Internet Security/Safety” (Metropolitan Police Department) (in Japanese)

<http://www.npa.go.jp/cybersafety/>

“The Consultation Window for Cyber Crimes in the Police Departments in Major Cities” (Metropolitan Police Department) (in Japanese)

<http://www.npa.go.jp/cyber/soudan.htm>

(4) The Countermeasures for the Game Site Manager’s Side

The damage cause for account hacking may be existed in game site manager’s side. In that case, following methods can be considered.

Method 1: <Attack (s) to the server in the game site manager side (Brute Force Attack, etc.)>

In case the server managed by the game site manager does not furnish enough security (resistance) against massive login-attempt attack (Brute Force Attack, etc.), malicious intent who fraudulently logged in to the server may steal items for online game users.

Method 2: <Attack (s) against the vulnerability (ies) in the website for the game site manager’s side>

The server managed by the game site manager conducted by the attack (s) exploiting vulnerability (ies) in the OSs and applications and the individual information for the online game users will be eavesdropped by the malicious intent intruded to the server.

Accordingly, the game site manager should recognize that the server may be targeted by the attack (s) with the methods described above: as for the Method 1 above, it is effective to limit the number for the failure in the login attempts, installation of intrusion detection system such as IDS/IPS, etc. As for the Method 2, be sure to check if unnecessary functions and services are in operation, vulnerability (ies) in OSs and applications are sufficiently resolved, and the server being managed is sufficiently configured, etc. one more time.

<Reference>

“Guide for Vulnerability (ies) Responses for Web Site Managers” (IPA) (in Japanese)

http://www.ipa.go.jp/security/fy19/reports/vuln_handling/

“How to Create Secure/Safe Website” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/vuln/websecurity.html>

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

The detection number of virus ^(*) in September was about **76T**: the number was shifted maintaining in the same level of 76T in August. In addition, the reported number of virus ^(**) in September was **1,301**: 6.5% increased from 1,222 in August.

^(*) 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 September, the reported number was 1,301 and the aggregated virus count was about 76T.

The worst detection number was **W32/Netsky** with about **68T**: **W32/Mydoom** with about **2.7T** and **W32/Mytob** with about **2.6T** followed.

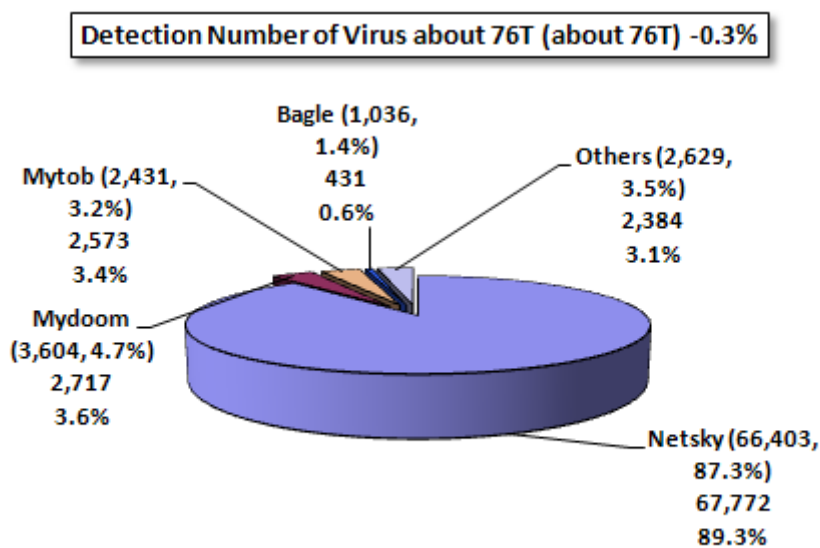


Chart 2-1: Detection Number of Virus

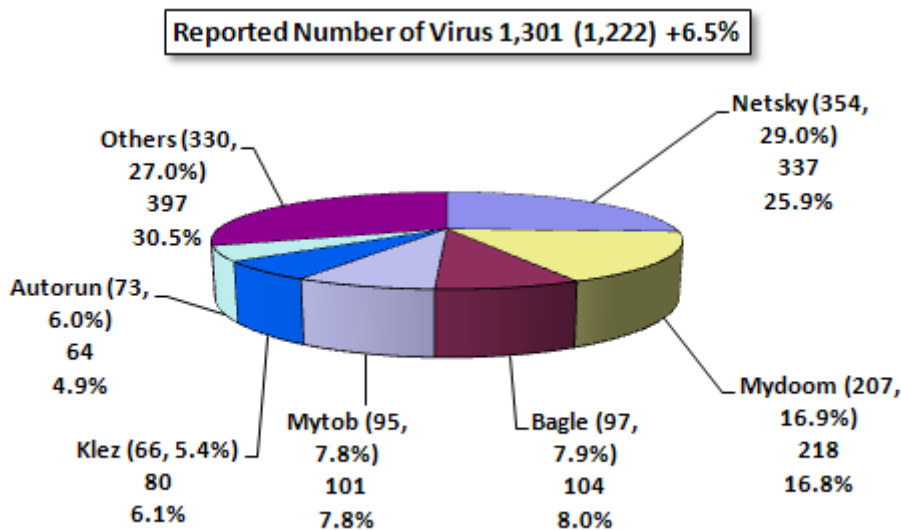


Chart 2-2: Reported Number of Virus

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

	Apr.	May	June	July	Aug.	Sep.
Total for Reported ^(a)	9	8	7	14	20	11
Damaged ^(b)	6	6	6	6	12	8
Not Damaged ^(c)	3	2	1	8	8	3
Total for Consultation ^(d)	39	45	35	24	39	44
Damaged ^(e)	11	16	9	3	17	13
Not Damaged ^(f)	28	29	26	21	22	31
Grand Total ^(a + d)	48	53	42	38	59	55
Damaged ^(b + e)	17	22	15	9	29	21
Not Damaged ^(c + f)	31	31	27	29	30	34

(1) Reporting Status for Unauthorized Computer Access

Reported number in September was **11**: Of **8** was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was **44** (of **4** were also counted as reported number): Of **13** was the number actually damaged.

(3) Status of Damage

The breakdown for the damage reports were intrusion with 3, masquerading with 4 and others (damaged) with 1.

The damage relevant to intrusion was that the credit card information stored within the server was browsed/stolen by SQL^(*) Injection^(*) Attack with 2; webpage alteration (embedding of malicious tag) with 1. The damage cause relevant to intrusion was that the vulnerability (ies) in web application (s) was exploited with 2, etc. (the cause for the other one has not yet identified.) The damage relevant to “masquerading” was that someone logged in to the online site (s) spoofing to be the legitimate user used online services (online games) fraudulently with 4.

*SQL (Structured Query Language): The query language used for data operation and definition in the relational database management system (RDBMS).

*SQL Injection: The attacking method which browse/overwrite data within database fraudulently by exploiting the defects in the program (s) accessing to the database.

(4) Damage Instance

[Intrusion]

- (i) The information stored in the database may have been browsed by blind SQL Injection Attack...

Instance	<ul style="list-style-type: none"> -“Number of SQL injection attack to the web server was monitored” so communicated by the organization where manages our division’s network. -Study was conducted with the simple log detection tool by a maintenance company, but none of anomaly was detected. However, fraudulent computer access to our database was detected by precise analysis conducted by the other maintenance company. According to it, the ID and the password to be used for log-in to the site may have been deviated. -Because of the vulnerability (ies) in cgi which was operated within the web server, malicious intent could successfully conduct SQL injection attack (s). In this case, Blind SQL injection attack method was used. -We’d conducted general anti-vulnerability measures for that cgi, but the countermeasures against the Blind SQL infection attack was not sufficiently considered.
----------	---

- (ii) Credit card information was stolen by SQL infection attack and fraudulently used...

Instance	<ul style="list-style-type: none"> -I am running an online shopping site. One of credit card companies referred to us of the fraudulent use of their card so that we checked our web server, but none of anomaly was defined. However, another, but similar inquiries came subsequently so that we asked one of security professionals to check access logs: according to him/her, it was realized that the SQL injection attack was successfully conducted and the malicious intent easily accessed to the credit card information stored in the database operated by that server. -Since I’d used web application package to construct the online shopping site, but the developer repeatedly responded that there is none of vulnerability in their products. However, it was realized that there is vulnerability in that application thereafter. -Accordingly, reopening the site in the current operational environment was stopped. As of now, I am considering the use of the other ASP service for which security requirements are ensured.
----------	---

IV. Accepting Status of Consultation

The gross number of consultation in September was 1,653. Of the consultation relevant to “**One-click Billing Fraud**” was **650** (August: 654). The consultation relevant to “**Hard selling of falsified anti-virus software**” was **6** (August: 1), the consultation relevant to “**Winny**” with **0** (August: 3), were also realized. (The consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” was **0** (August: 2).

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

	April	May	June	July	August	Sept.
Total	1,668	1,765	1,898	1,708	1,792	1,653
Automatic Response System	962	992	1,081	923	1,015	915
Telephone	651	710	777	736	702	676
e-mail	55	58	37	47	68	60
Fax, Others	0	5	3	2	7	2

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

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

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

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

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

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

*The Total case number includes the number in Consultation ⁽⁴⁾ column of the Chart in the “III. Reporting Status of Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

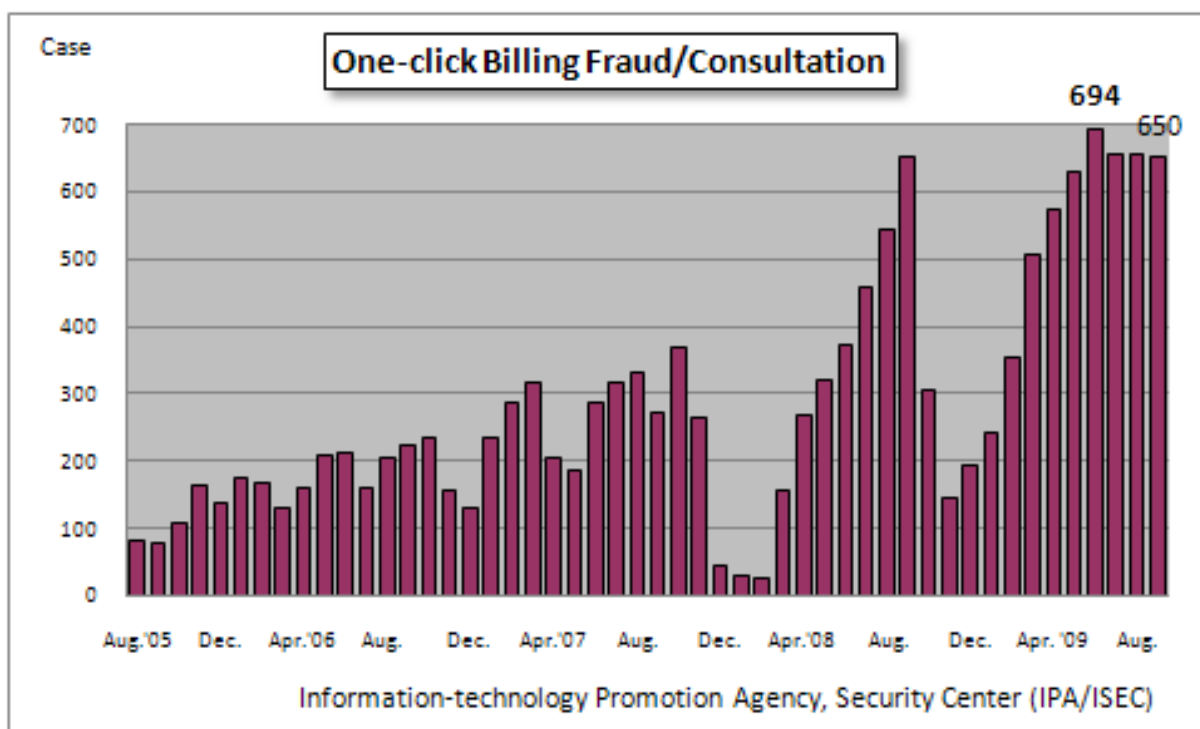


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

- (i) Billing statement was appeared when I accessed to the site someone told me while we were chatting ...?

<p>Consultation</p>	<p><Consultation from a child>He/she chatted with someone who'd met on the Internet. The person (kindly?) told him/her the link to one site (i.e., URL) so that he/she continually clicked "Yes" and eventually he/she was sent to an adult site. Though he/she rebooted to the computer, each time the billing statement to the adult site was appeared, thereafter. The computer was infected by the virus which displays such billing statement over and over even though the computer would be rebooted.</p>
<p>Response</p>	<p>Sad to say that there is number of malicious users who attempt to deceive/fool the other side of users on the Internet. Specifically, children are easily getting their targets. Accordingly, it is utmost important to block (filtering) the hazardous sites as well as installing anti-virus software for those families who share one computer and/or let their kids to use the computer. Simple filtering software is available, but such function sometimes appended on to the general anti-virus software or the function may be included in provider's services.</p> <p><Reference> Reminder for July 2007 "Firewall Protects Your Computer, Security in Your Mind Protects Your Sound State" http://www.ipa.go.jp/security/english/virus/press/200707/E_PR200707.html</p>

- (ii) Virus was infected to iPod ...?

<p>Consultation</p>	<p>I downloaded some music files from the site in China. It might be imagine, but my computer seemed to behave differently, thereafter. According to one of consultants, I was suggested to initialize my computer: in prior to that, I used iPod (mobile music player) to back up data to the other computer. I copied files to the iPod and connected it to the other computer, then, its anti-virus software detected virus. Had the virus being infected to the iPod?</p>
<p>Response</p>	<p>In this case, some virus file was simply located to the iPod so that the virus in the iPod does not cause damage to the iPod itself. Rather, it seems that some virus has been infected to your computer for some reason. The virus is the one which enlarges infection via outside memory media such as USB memory, etc. so that the virus was copied to the iPod as well. In this case, you can not only be a casualty, but also be a criminal by distributing virus while you do not know: accordingly, be sure to conduct your anti-virus measures for your computer thoroughly for your further security. In addition, it is also helpful to disable the "automatic execution function" on Windows to prevent from the Windows automatically running.</p> <p><Reference> Reminder for April 2009 "Are You Always Recognizing the Security Measures for USB Memory?" http://www.ipa.go.jp/security/english/virus/press/200904/E_PR200904.html</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in September was **160,487** for the 10 monitoring points and the gross number of source* was **58,770**. That is, the number of access was **535** from **196** 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.

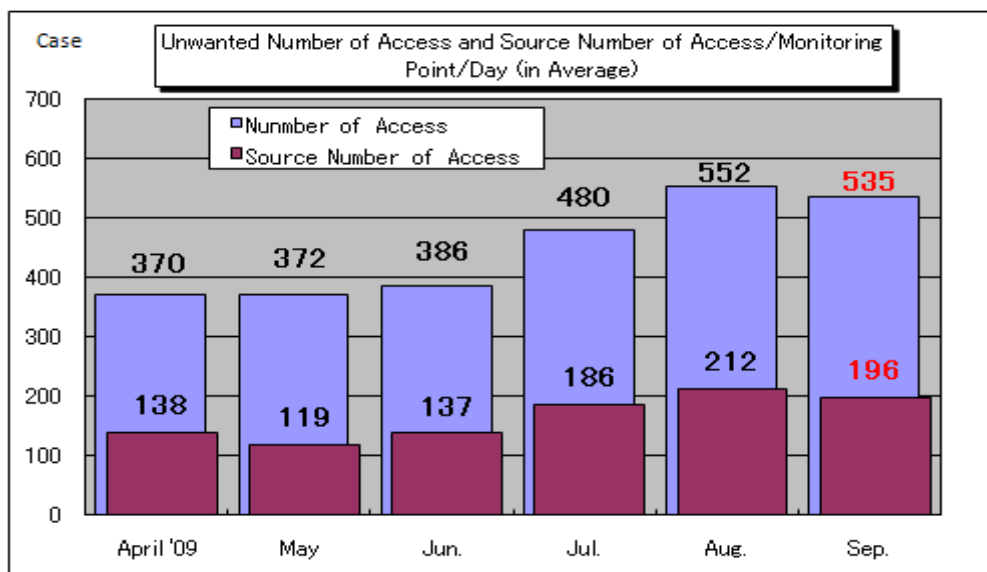


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access (average) and the source number of access (average)/monitoring point/day from April to September 2009. According to this chart, both the unwanted (one-sided) number of accesses were subtly decreased from the ones in August.

The Chart 5-2 shows the comparison in unwanted (one-sided) number of accesses classified by destination (by port) in August and September. There were none of the port from which/to which accesses drastically shifted. The access to the port 445/tcp which was continually increasing from 4 months ago was turned to decreasing from September.

In addition, the access to the port 1080/tcp which never been listed in the one of frequently accessed ports could often be observed. This was the access from one of the sources in China for which access was continually observed from September 7 (please refer to the Chart 5-3): it could be realized that the same source accessing to the port 1025/tcp was also observed simultaneously. These accesses were monitored by of 7 monitoring points out of 10 in TALOT2 system; accordingly, it could be assumed that the same event may have been caused extensively (please refer to the Chart 5-4 and 5-5). The port 1080/tcp is the general port to be used by SOCKS server* and the port 1025/tcp is the renowned port being attacked by the virus which exploiting vulnerability (ies) in Windows in 2005 (MS05-051). The reason why the source was continually accessed to these ports was unknown.

SOCKS server*: the one of proxy servers which conducts communication to the Internet on behalf of corporate LAN, etc.

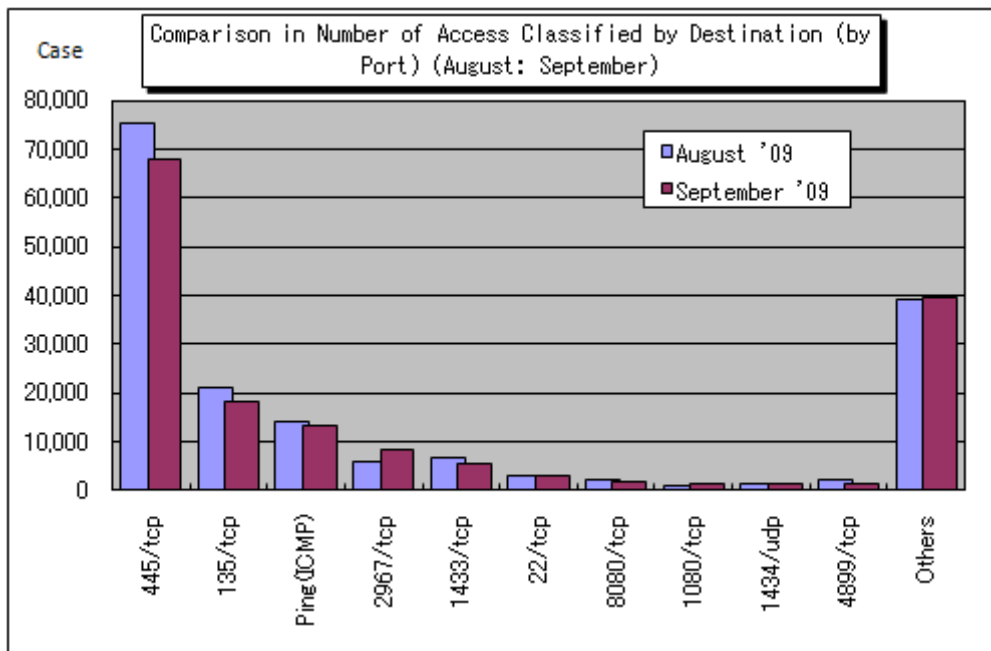


Chart 5-2: Comparison in Number of Access Classified by Destination (by Port) (August: September)

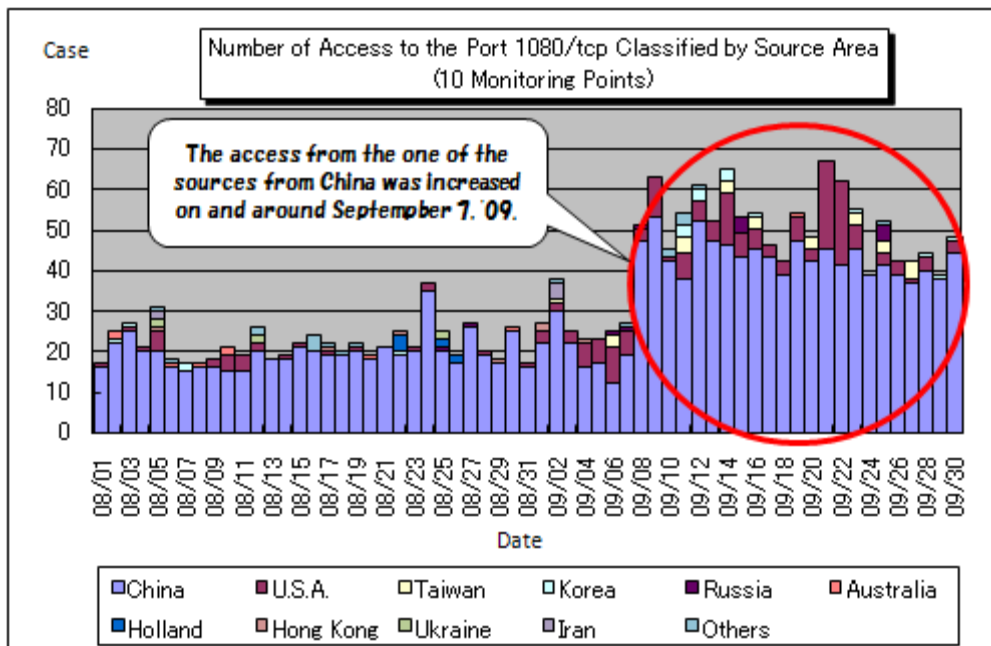


Chart 5-3: Number of Access to the Port 1080/tcp Classified by Source Area (10 Monitoring Points Total)

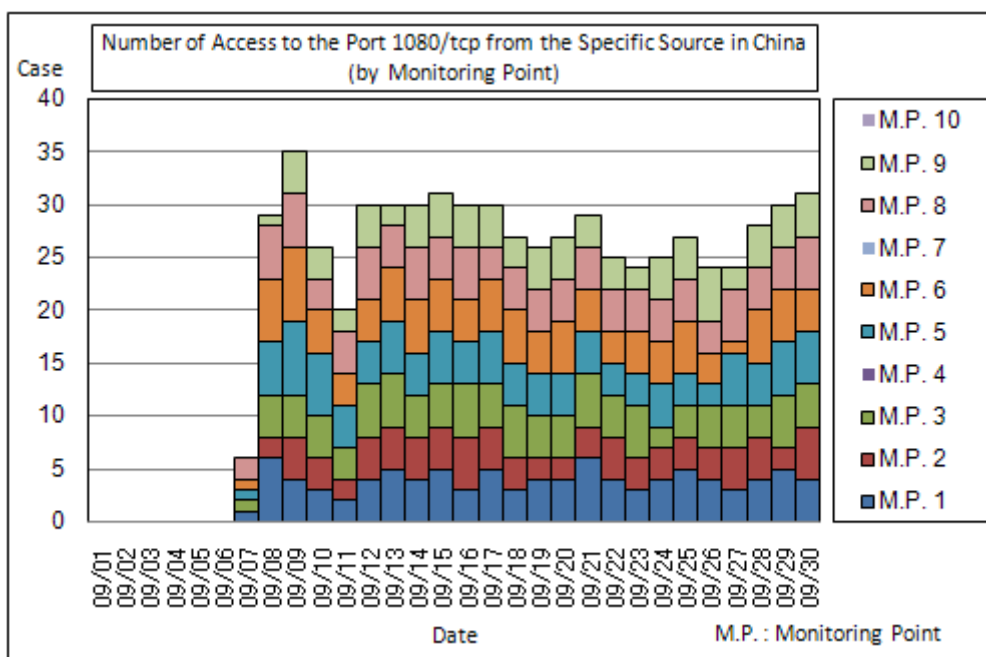


Chart 5-4: Number of Access to the Port 1080/tcp from the Specific Source in China (by Monitoring Point)

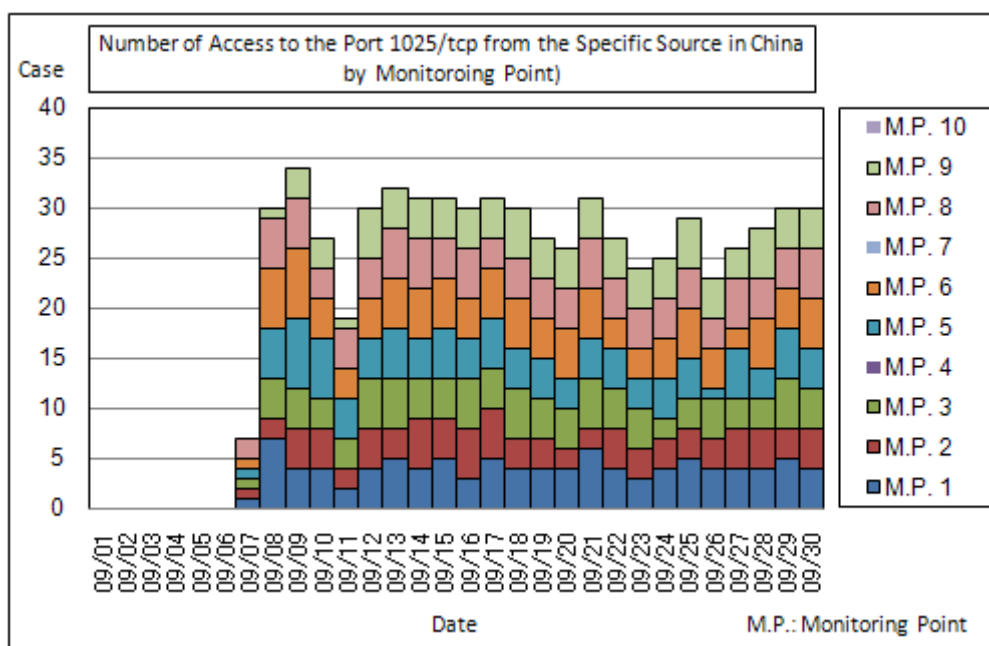


Chart 5-5: Number of Access to the Port 1025/tcp from the Specific Source in China (by Monitoring Point)

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

Attachment_3: Accessing Status Captured by the Internet Monitoring (TALOT2)
<http://www.ipa.go.jp/security/english/virus/press/2009/documents/TALOT2-0909.pdf>

Summary Reporting Status for Computer Virus/Unauthorized Computer Access for July
<http://www.ipa.go.jp/security/english/virus/press/2009/documents/summary0909.pdf>

Attachment_1 Computer Virus Incident Report
<http://www.ipa.go.jp/security/english/virus/press/2009/documents/virus0909.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/crack0909.pdf>

Attachment_4 Computer virus Incident Report for the 3rd Quarter (July to September)

<http://www.ipa.go.jp/security/english/virus/press/200909/documents/virus2009-3Q.pdf>

Attachment_5 Unauthorized Computer Access Incident Report for the 3rd Quarter (July to September)

<http://www.ipa.go.jp/security/english/virus/press/200909/documents/ua2009-3Q.pdf>

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

JPCERT/Coordination Center (CC):

<http://www.jpCERT.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