Press Release
August 12, 2011
Information-technology Promotion Agency, Japan

Computer Virus/Unauthorized Computer Access Incident Report *- July 2011 -*

This is the summary of computer virus/unauthorized computer access incident report for July 2011, compiled by Information-technology Promotion Agency, Japan (IPA).

I. Reminder for this Month

"Let's use your smart phone in a secure manner!"

In February 2011, IPA released a reminder[*1] about a computer virus that targets smart phones (hereinafter referred to as smart-phone-targeting virus). Ever since, new types of such virus have emerged one after another, posing an increasing risk of virus infections to smart phone users.
Further, from the virus reports submitted recently to IPA, we could see the emergence of smart-phone-targeting viruses (especially for Android terminal).
Given this situation, this report explains virus situation surrounding smart phones as well as specific measures to take for the safe use of smart phones.

*1 Reminder of the February 2011 issue "Watch out for smart-phone-targeting viruses"
http://www.ipa.go.jp/security/english/virus/press/201101/E_PR201101.html

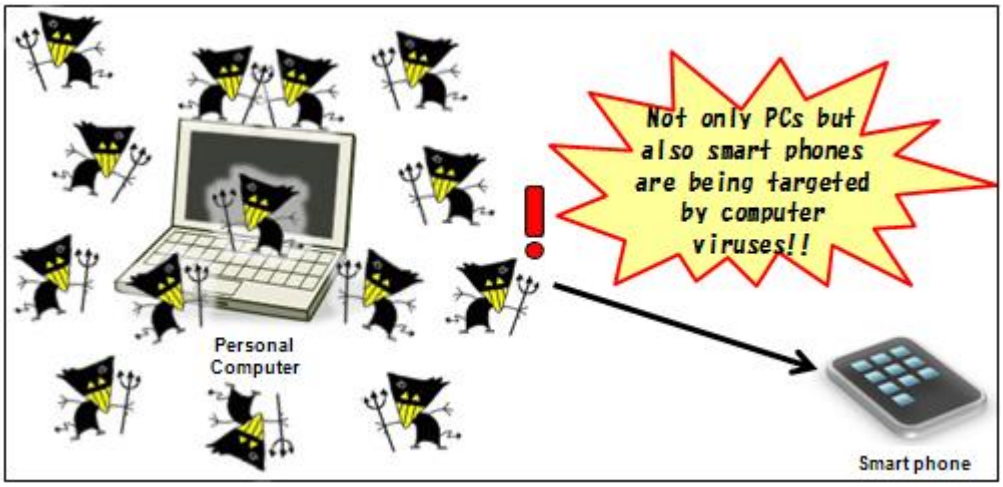


Figure 1-1: Image of a Smart Phone Being Targeted by a Virus

(1) Recent Virus Situation Surrounding Smart Phones

Table 1-1 shows a list of Android-targeting viruses that have been reported to IPA.

Table 1-1: A List of Android-Targeting Viruses that Have Been Reported to IPA

Reported period	Name	Characteristics
Mar. 2011	AndroidOS/Lotoor [DroidDream]	By downloading it from a Website, the Android terminal is infected. It collects information stored on the terminal and transfers it to an outside party.
Jun. 2011	AndroidOS/Lightdd	After the infection, it collects information stored on the Android terminal and transfers it to an outside party.
Jun. 2011	AndroidOS/Smspacem	After the infection, it attempts to send SMS[*2] message to the addresses registered in the Android terminal's address book.
Jun. 2011	AndroidOS/Smstibook	After the infection, it attempts to send premium SMS[*3] message to a number specified in advance.

*2 SMS (Short Message Service): A service that allows an e-mail with a short message to be sent/received between cell-phones.

*3 Premium SMS: A type of SMS in which the one receiving a SMS message sent from a sender benefits.

In this way, this year, smart-phone-targeting viruses have been detected one after another, posing an increasing risk of virus infections to smart phone users.

Possible damages caused by the infection of smart-phone-targeting viruses are as follows:

- Data and critical information (including location information identified by GPS*4 and other personal information) that is stored on the smart phone might be transferred to a third party with malicious intent;
- The smart phone might be taken over and used freely by a third party with malicious intent;
- The smart phone might be incorporated into a Botnet*5 and used as a tool for carrying out a cyber attack against a specific organization or other crimes without the user's knowledge.

*4 GPS (Global Positioning System): A system to determine the location of an object on the globe using an artificial satellite's airwave.

*5 Botnet: A network consisting of a large number of computers that are infected with a virus called bot. It is used by an attacker to carry out an attack from a remote site against its target

(2) Smart-phone-targeting Viruses That were Reported to IPA

Figure 1-2 shows a chart of the number of detected smart-phone-targeting viruses that were reported to IPA from March to July 2011.

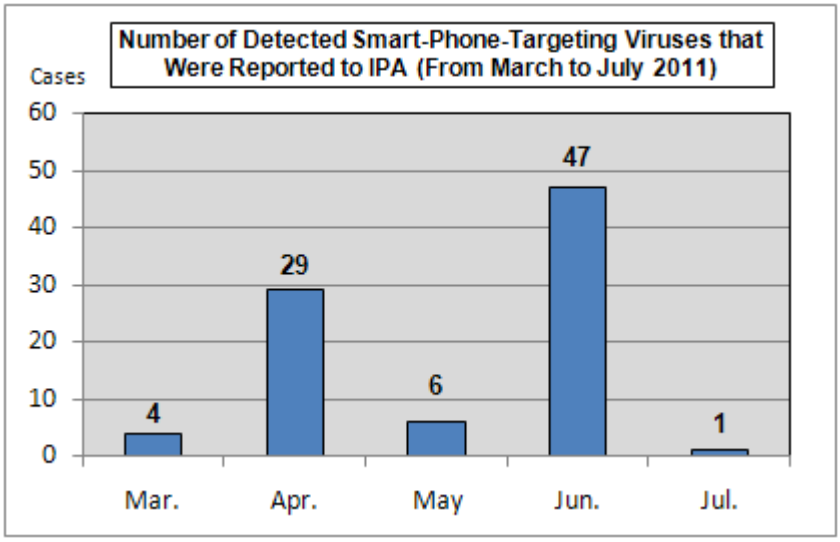


Figure 1-2: Number of Detected Smart-phone-targeting Viruses that were Reported to IPA

All of these viruses are not the ones detected on smart phones but PCs equipped with Windows, etc., at the time of receipt of an e-mail, etc. Those viruses were attached to an e-mail so that smart phones that open the e-mail are infected with them. Because such e-mail was sent to unspecified number of people, it was also received by PCs. Further, because security software for Android terminals is not so popular, there has been no report on the detection of a virus on smart phones. All of the smart-phone-targeting viruses that were reported to IPA from March to July 2011 were designed to target Android terminals.

If a smart phone receives an e-mail to which a virus-infected application is attached, it starts behaving oddly and how it behaves vary depending on its model and OS. **For Android terminals, if the user pushes the "Install" button that is displayed when he/she opened that e-mail, the installation process for the application starts and the terminal is infected with the virus.** So, you need to exercise care in handling e-mails. Figure 1-3 shows the screen image of a smart phone (terminal name: GALAXY Tab/OS, version: Android 2.2) viewing an e-mail to which an Android application (.apk file) is attached.

Figure 1-3: Screen Image of a Smart Phone Viewing an E-mail to which an Android Application is Attached

(3) Six Recommendations for the Safe Use of Smart Phones

Given the current status of smart-phone-targeting viruses, IPA organized six recommendations for the secure use of smart phones, taking into account countermeasures against viruses and attacks that exploit vulnerabilities. Please make them use of as a guideline for the secure use of smart phones (See Figure 1-4).

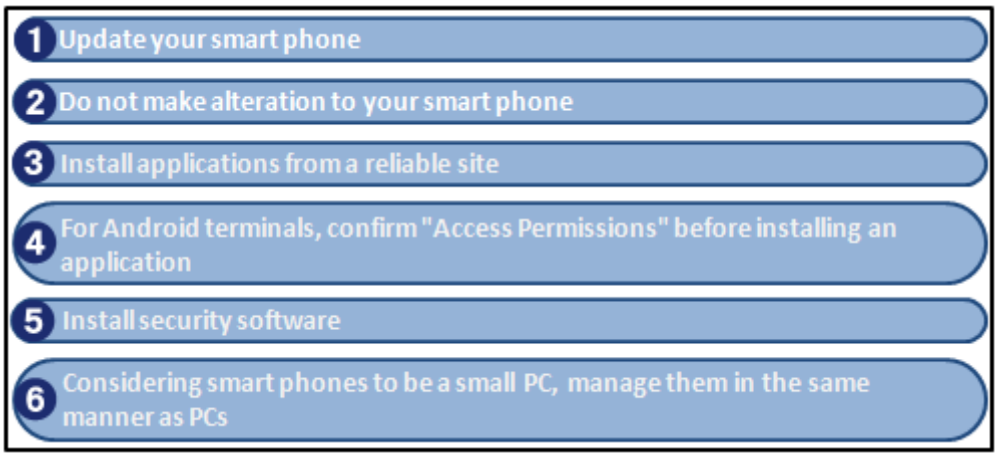


Figure 1-4: Six Recommendations for the Secure Use of Smart Phones

Detailed explanation for each item is as follows:

[I] Update your smart phone

When an update for the OS was released by its provider, apply it promptly. If your smart phone is left un-updated, as with PCs, it is more likely to receive an attack that exploits its vulnerability. It is also important to understand update procedure. Update procedure may vary depending on the distributor or manufacture. To ensure that update is performed properly, check the instruction manual, etc. for correct procedure and perform the update.

[II] Do not make alteration to your smart phone

Do not make any alterations to your smart phone. In this context, alterations refer to such act as Jailbreak on an iPhone terminal or takeover of root privilege on an Android terminal. Among the viruses that run on smart phones, some of them have been confirmed to infect only altered smart phones. Such actions may result in increasing the risk of virus infections by yourself, so do not make alterations to your smart phone.

[III] Install applications from a reliable site

For applications you are going to use on your smart phone, install them from a reliable site. For iPhone, visit Apple's "App Store" and for Android terminals, visit Google's "Android Market" which conducts screening of applications and the removal of illegal applications.

[IV] For Android terminals, confirm "Access Permissions" before installing an application

For Android terminals, when you install an application, be sure to look through the list of "Access Permission (which defines which information/functions of the Android terminal the application are going to access)" that is displayed (see Figure 1-5). Among the Android-targeting viruses detected in the past, there was the one that requests questionable access permissions irrelevant to its application type in order to steal personal information. For example, a wallpaper application asking for the permission to "read contact information", with which the application can access the contents of the address book and call logs. When you install an application on your Android terminal, if you feel suspicious about requested access permissions, do not install that application.

Figure 1-5: Display Screen Image for "Access Permissions"

[V] Install security software

For smart phones, particularly for Android terminals, a flood of security software has been released by major antivirus software vendors since the beginning of 2011. So now we have a wide range of choice. In regard to Android terminals, by exercising care with the issues described in [iv], users can mitigate the risk of virus infections to some extent but not to zero. In order to further mitigate the risk of virus infections, install security software.

[VI] Considering smart phones to be a small PC, manage them in the same manner as PCs

When making use of a smart phone within an enterprise, the enterprise should establish rules on the use, scope of accessible information, scope of storable information, and how to respond to loss or theft of that smart phone. It is recommended to set up a mechanism for enterprises to enforce the update of the OS installed on the smart phone and to restrict installable applications through Mobile Device Management (MDM).

II. Computer Virus Reported – for more details, please refer to Attachment 1 –

(1) Computer Virus Reported

While the virus detection count [*1] in July was **about 23,000**, down 39.4 percent from about 38,000 in June, the virus report count [*2] in July was **1,064,** down 12.0 percent from the June level (**1,209**).

*1 Virus detection count: indicates how many times a specific virus appeared in the reports submitted, or the aggregate virus detection counts for a specific period.

*2 Virus report count: indicates how many reports on a specific virus were submitted. If the same type of viruses were reported by the same person with the same detection day, they are counted as one report regarding the virus of that sort.

* In July, the virus report count, which was obtained by consolidating about 23,000 virus detection reports, was 1,064.

W32/Netsky marked the highest detection count at **about 10,000**, followed by **W32/ Mydoom** at **about 9,500** and **W32/ Autorun** at **about 1,500**.

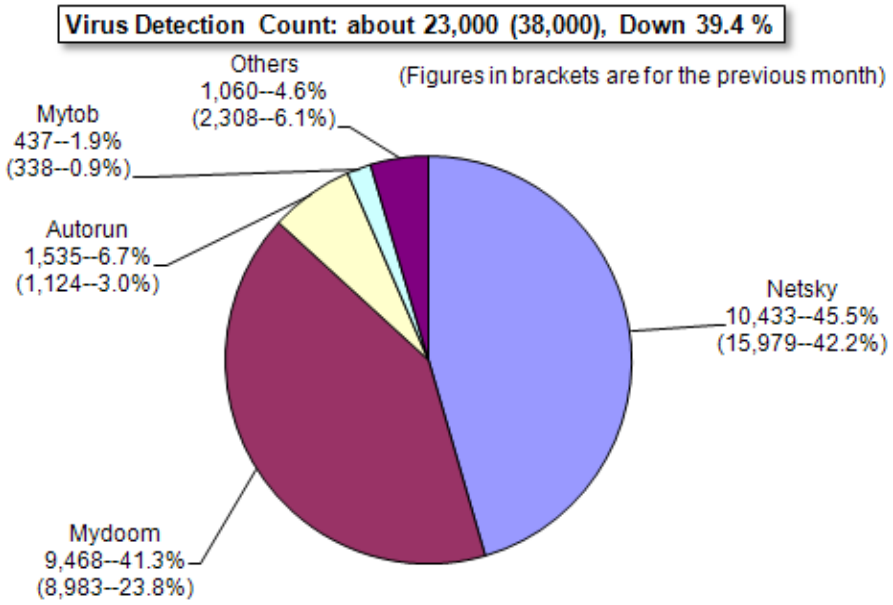


Figure 2-1: Virus Detection Count

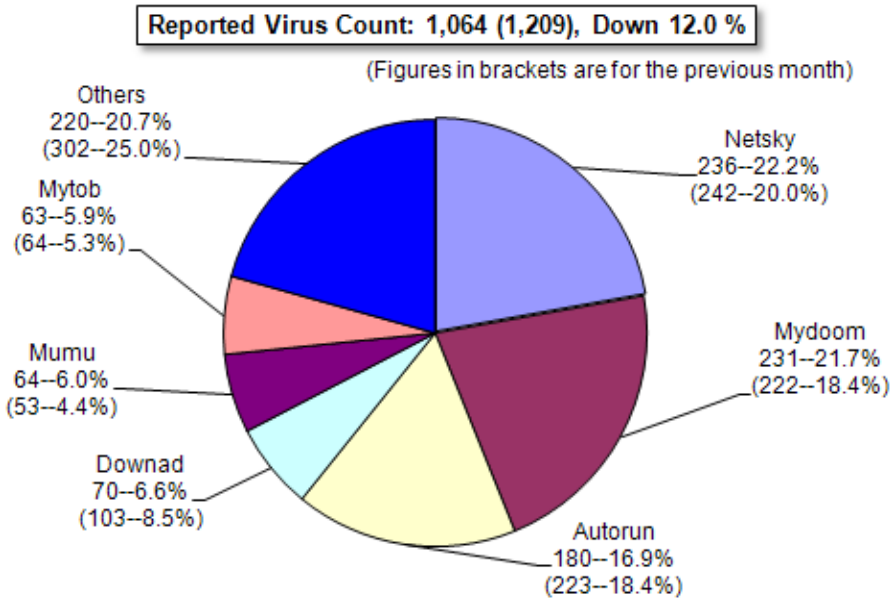


Figure 2-2: Virus Report Count

（2） Malicious Programs Detected

In July, there was no remarkable change (See Figure 2-3).

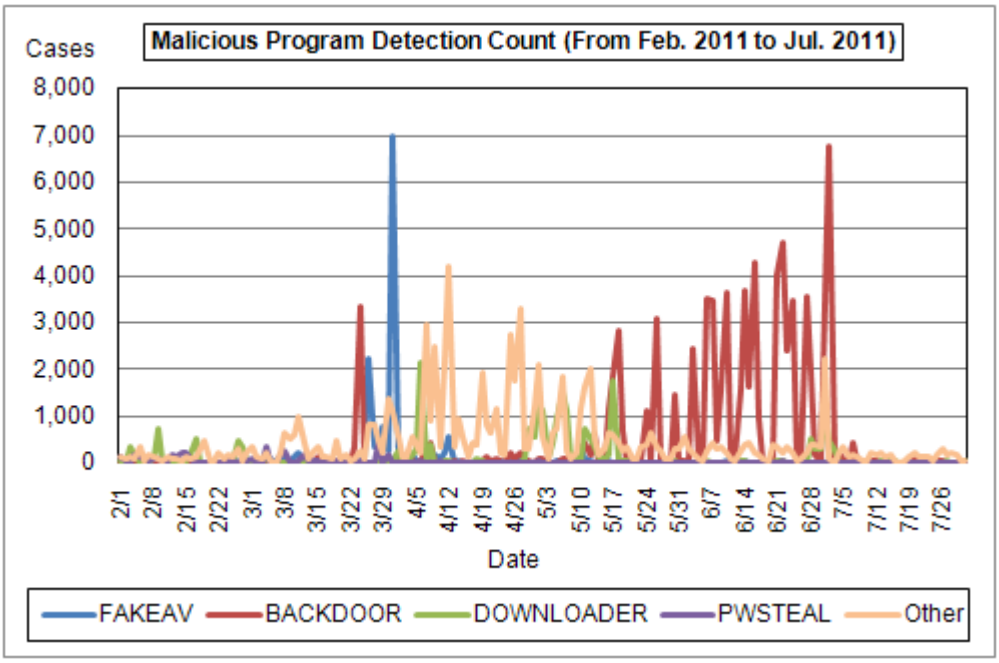


Figure 2-3: Malicious Program Detection Count

III. Unauthorized Computer Access Reported (including Consultations) – *for more detail, please refer to Attachment 2* –

Table 3-1: Unauthorized Computer Access Reported (including Consultations)

	Feb. '11	Mar.	Apr.	May	Jun.	Jul.
Total for Reported [a]	**10**	**6**	**5**	**7**	**9**	**8**
Damaged [b]	5	6	5	6	9	5
Not Damaged [c]	5	0	0	1	0	3
Total for Consultation [d]	**23**	**45**	**38**	**55**	**32**	**47**
Damaged [e]	6	10	10	14	7	15
Not Damaged [f]	17	35	28	41	25	32
Grand Total [a + d]	**33**	**51**	**43**	**62**	**41**	**55**
Damaged [b + e]	11	16	15	20	16	20
Not Damaged [c + f]	22	35	28	42	25	35

（1）Unauthorized Computer Access Reported

The report count for unauthorized computer access in July was 8, 5 of which reportedly had certain damages.

（2）Unauthorized Computer Access and Other Related Problems Consulted

The consultation count for unauthorized computer access and other related problems was 47. 15 of them reportedly had certain damages.

（3）Damages Caused

The breakdown of the damage reports were: **intrusion (4); spoofing (1).**

Damages caused by "intrusion" were: a database's configuration information being stolen (1); a tool to attack an external site being embedded in a server, which in turn used as a stepping stone (2); a file being uploaded without permission (1). Causes of "intrusion" were: improper setting (3, two of them involved improper setting for access restriction and one involved non-routinely-used-but-then-activated function being exploited); and other cases remain unknown.

Damages caused by "spoofing" were: an IP telephone service being used by someone who successfully impersonated a legitimate user and logged on (1).

（4）Damage Instance

［Intrusion］

（i）Our server's improper setting was exploited by an attacker to break into it and place a file

Instance	- I was notified by an external party, "we've detected an upload communication against your Web server." - Upon investigating the server, I found an unknown file in the Web application directory on the server. - The server was using Tomcat and Tomcat's Web application manager feature was enabled. Using this feature, the attacker uploaded that file on the server. - As a post-incident response, I removed Tomcat's Web application manager feature as I felt it no-longer-needed.

［Malicious Program Embedded］

（ii）An unknown rule was added to our firewall

Instance	- I found a firewall setting that violates company's regulations. A rule had been added to the firewall so that it allows for any communications to an in-house server. - Upon investigating the server, I found that a malicious program had been embedded into the server, which in turn had used for SSH scan against external servers. - As a post-incident response, the company changed the firewall's administrator's password and reviewed the application procedures for making changes to firewalls and established measures to have its staff follow those procedures. - This case is still under investigation, but it may have been caused by an inside man.

IV. Virus and Unauthorized Computer Access related Consultations

The total number of consultations in July was **1,490**. **461** of which were related to **"One-Click Billing"** (compared to 511 in June); **8** to **"Fake Security Software"** (compared to 11 in June); **7** to **"Winny"** (compared to 7 in June); **2** to **"A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data"** (compared to 6 in June)

Table 4-1: Total Number of Consultations Handled by IPA over the Past Six Months

	Feb. '11	Mar.	Apr.	May	Jun.	Jul.
Total	**1,521**	**1,723**	**1,608**	**1,640**	**1,692**	**1,490**
Automatic Response System	892	1,106	997	950	999	889
Telephone	570	551	555	620	639	540
e-mail	53	58	50	62	50	54
Fax, Others	6	8	6	8	4	7

* IPA set up "Worry-Free Information Security Consultation Service" that provides consultation/advises for computer virus, unauthorized computer access, problems related to Winny as well as overall information security.

E-mail address: anshin@ipa.go.jp
Tel.: +81-3-5978-7509 (24-Hour Automatic Response; Consultations are provided by IPA Security Center personnel and 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
*Total Number includes the number in the Consultation [(d)] column in the Table 3-1, "III. Unauthorized Computer Access Reported (including Consultations)".

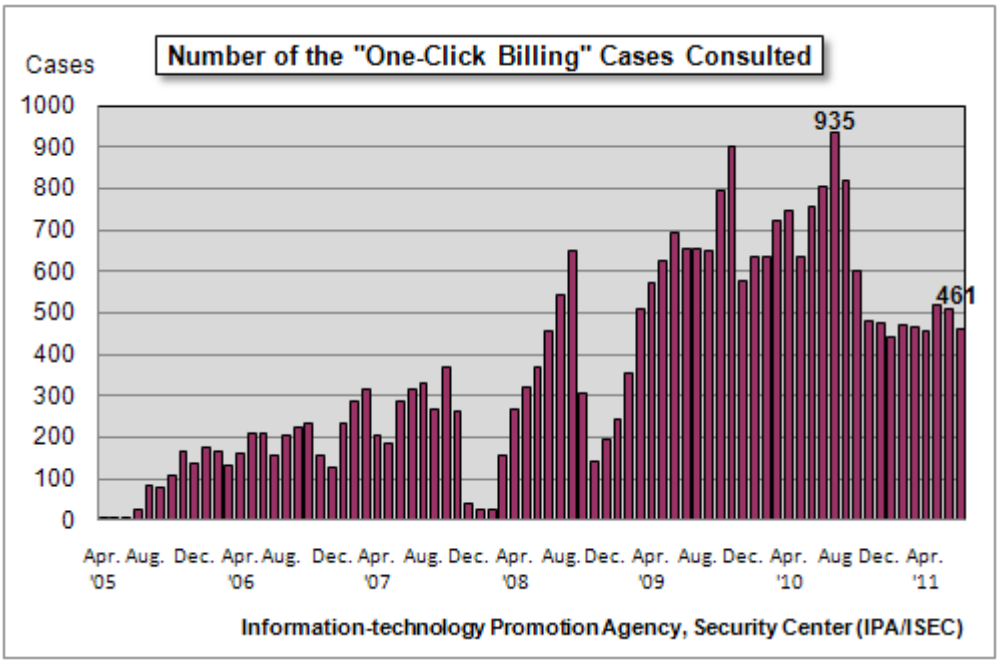
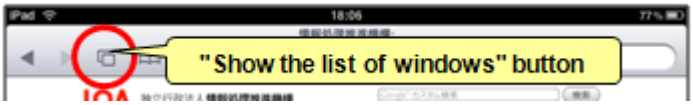


Figure 4-1: Number of the "One-Click Billing" Cases Consulted

Major consultation instances are as follows:

(i) When I accessed a sexually explicit site from my iPad, the site's page appeared and it does not disappear

What was consulted	When I accessed a sexually explicit site from my iPad, the site's page appeared and it does not disappear as if stuck to the screen. Although I restarted my iPad, it still remains on the screen. Does this mean that what is called one-click billing on PCs is occurring on my iPad? In the case of iPad, how can I remove it?
Response	In this case, because information on the page in question remains in the cash or access history of Safari, which is a preinstalled browser for iPad, whenever Safari is opened, that information is loaded and the page is displayed. To resolve this situation, push the "Show the list of windows" button and push the "x" mark on the upper left of the window you want to close.  **Figure 4-2: Upper Part of the Screen of iPad's Safari** Although no case has been confirmed by IPA in which a billing screen is displayed on iPad, a similar phenomenon might occur on iPad in the future. So, exercise care in accessing Websites. <Reference> IPA - "[Security Alert] "An increasing number of inquires were made about one-click billing! The first step for PC users is to know its mechanism!" http://www.ipa.go.jp/security/topics/alert20080909.html (in Japanese)

(ii) In mistake for IPA, I asked another organization for the response to one-click billing

What was consulted	Suddenly, a sexually explicit site's billing screen appeared and it did not disappear. When I consulted the consumer affairs bureau, I was advised to visit IPA's Website for the steps to remove the billing screen. So I searched "IPA" on a search site and clicked on an URL listed at the top of the page as the search result, assuming that this was IPA's. Later, I found that this was another organization's URL. Although it was a fee-based service, I used it as I thought my problem could be solved with just one call. I followed their instruction and was able to remove the billing screen. But when I checked again for the Website, I was convinced that it was not IPA's. I'm sure I searched "IPA". What's going on?

Response	The organization you asked for the response was irrelevant to IPA. When one performs a keyword search on a search site, the information one wants is not always listed at the top of the page. Depending on the search site, information provide by advertisers may appear at the top instead. When you perform a keyword search for information you want on a search site, confirm carefully the title, URL, description, etc. of each site listed and be careful not to access wrong information. For information on one-click billing provide by IPA, please refer to the Web page bellow. <Reference> IPA - "[Security Alert] "An increasing number of inquires were made about one-click billing! The first step for PC users is to know its mechanism!" http://www.ipa.go.jp/security/topics/alert20080909.html (in Japanese)

V. Access Status Captured by the Internet Fixed-Point Monitoring System (TALOT2) in July

According to the Internet Fixed-Point Monitoring System (TALOT2), **102,888** unwanted (one-sided) accesses were observed at ten monitoring points in July and the total number of sources* was **46,222**. This means on average, **343 accesses** form **154 sources** were observed at **one monitoring point per day**. (See Figure 5-1)

Total number of sources: indicates how many sources in total were observed by TALOT2. If multiple accesses from the same source were observed at the same monitoring point/port on the same day, they are considered one access from the specific source on that day.

Since the environment of each monitoring point for TALOT2 is equivalent to that of general Internet connection, an equal number of such accesses are thought to be made in the Internet users' system environment.

* For maintenance work, we shut down the systems on July 2. Therefore, the statistical information was derived from the data excluding that of July 2. Normally, the systems are in operation all times.

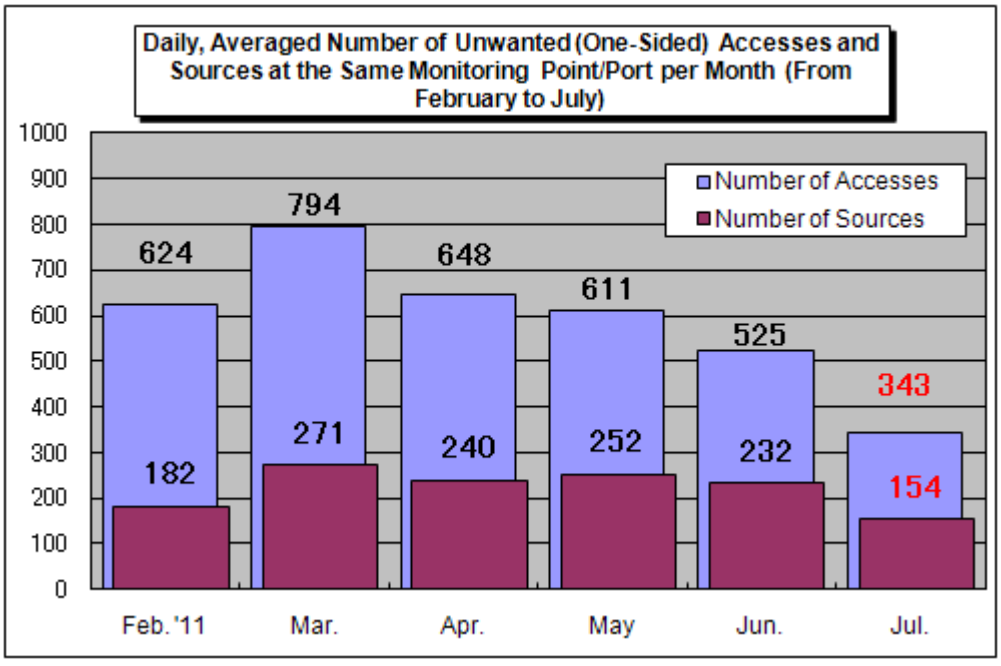


Figure 5-1: Daily, Averaged Number of Unwanted (One-Sided) Accesses and Sources at the Same Monitoring Point/Port per Month (From February to July)

The Figure 5-1 shows daily, averaged number of unwanted (one-sided) accesses and sources at the same monitoring point/port per month (from February 2011 to July 2011). As shown in this figure, the number of unwanted (one-sided) accesses in July has decreased significantly, compared to the June level.

The Figure 5-2 shows the July-over-June comparison results for the number of unwanted (one-sided) accesses, classified by destination (port type). As shown in this figure, compared to the June level, access to 445/tcp has decreased significantly while access to 11083/tcp has increased.

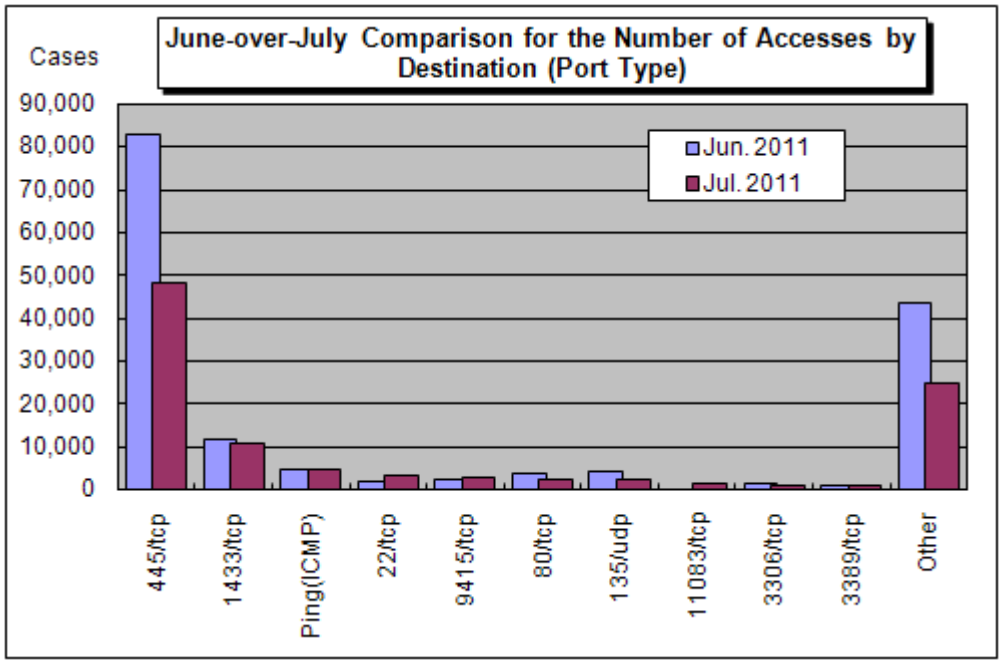


Figure 5-2: July-over-June Comparison for the Number of Accesses by Destination (Port Type)

Access to 11083/tcp began to be observed at a single monitoring point for TALOT2 after July 3 and such access was mainly made from the U.S and China (See Figure 5-3). It has yet to be identified why this port was accessed as it is not the one used by a specific application.

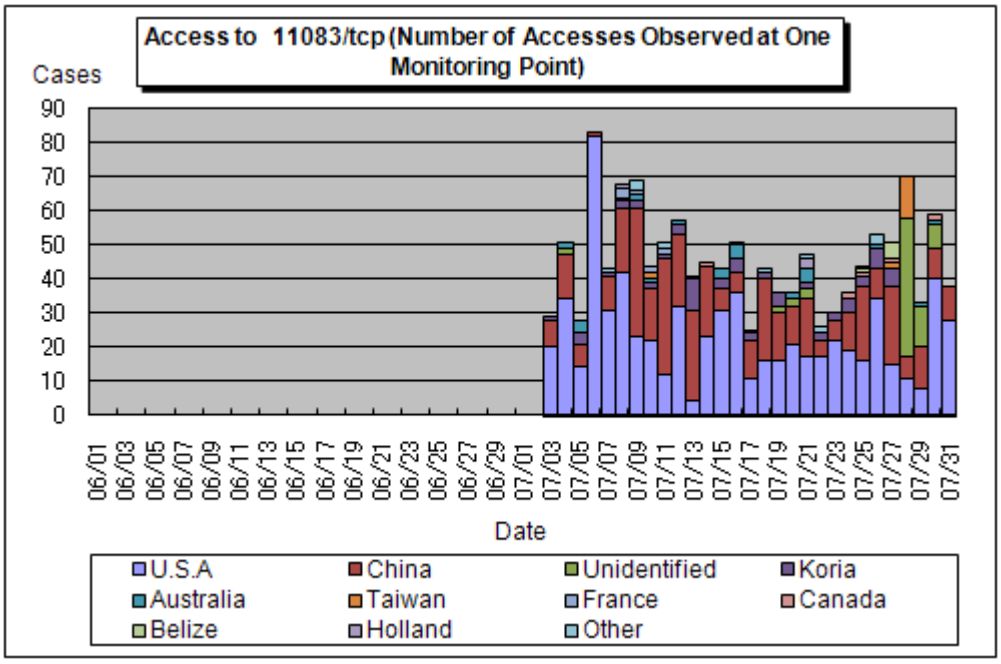


Figure 5-3: Access to 11083/tcp (Total Number of Accesses Observed at a Single Monitoring Point)

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

Attachment_3: Observations by the Internet Fixed-Point Monitoring System (TALOT2)
http://www.ipa.go.jp/security/english/virus/press/201107/documents/TALOT2-1107.pdf

Variety of statistical Information provided by the other organizations/vendors is available at the following sites:

JPCERT/Coordination Center (CC)：http://www.jpcert.or.jp/english/
@police：http://www.cyberpolice.go.jp/english/
Council of Anti-Phishing Japan: http://www.antiphishing.jp/ (in Japanese)
Symantec：http://www.symantec.com/
Trendmicro：http://us.trendmicro.com/us/home/
McAfee：http://www.mcafee.com/us/

Inquiries to:
IT Security Center, Information-technology Promotion Agency, Japan (IPA/ISEC)
Kagaya/Miyamoto
Tel.: +81-3-5978-7591
Fax: +81-3-5978-7518
E-mail: isec-info@ipa.go.jp