

Computer Virus/Unauthorized Computer Access Incident Report - January 2012 -

This is the summary of computer virus/unauthorized computer access incident report for January 2012, compiled by Information-technology Promotion Agency, Japan (IPA).

I. Reminder for this Month

"Watch Out for One-click Billing Fraud for Smartphone"

In 2012, an one-click billing fraud operator was arrested for "Unauthorized Creation of Electromagnetic Records" (so called "Use of a computer virus"), for which the PC of a Website visitor was infected with a virus and a billing screen for a sexually explicit site was pasted to the PC's screen and did not disappear.

Further, in the same month, there was a case in which a billing screen was continuously displayed on an Android OS smartphone, which was caused by a malicious application downloaded (for the sake of convenience, this is referred to as "virus" in the rest of this document), as in the case of one-click billing fraud on PCs. In this case, if a smartphone was infected with the virus, its phone number, e-mail addresses and other information are automatically passed on to the one-click billing fraud operator. As a result, the one-click billing fraud operator is able to contact the owner of the infected smartphone anytime, so if we compare PCs' damage situation with smartphones', we can see that techniques applied for smartphone are more malignant.

In this section, we make clear such techniques and explain measures to avoid suffering such damages.

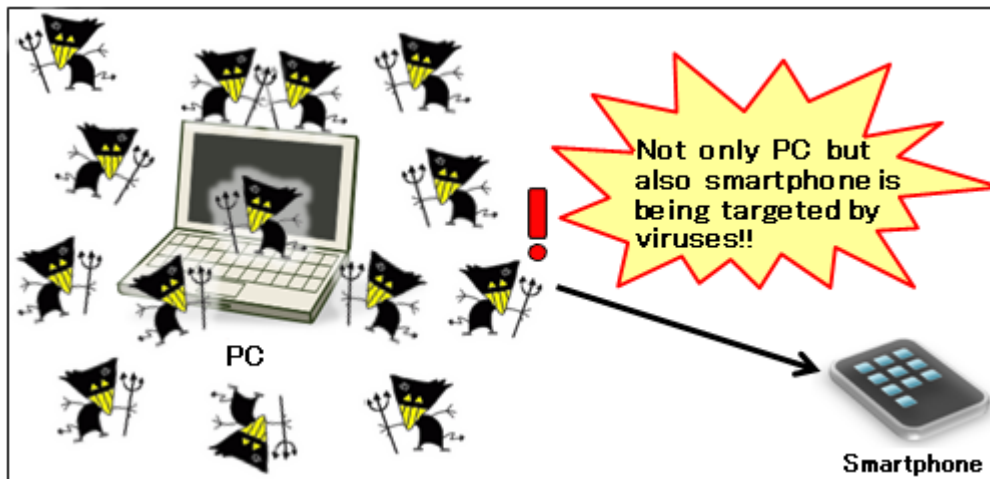


Figure1-1: Image of a Smartphone Being Targeted by Viruses

(1) Actual Damages Caused

[1] Guides to a Website that performs one-click billing fraud

Examples of techniques for guiding smartphone users to a Website that performs one-click billing fraud are as follows:

- Sends an unsolicited e-mail that contains a link (URL) to such Website to unspecified number of smartphone users so that those who are interested in it click it and are guided to the Website.
- Uses a technique called SEO (Search Engine Optimization) Poisoning to have the link to such Website appear at the top of a search site's search results so that those who are interested in it click it and are guided to the Website.

[II] Actual damages that IPA inspected

A technique for infecting smartphone with a virus, which IPA examined this time, takes the steps below. These steps are explained using the screens of "GALAXY Tab SC-01C (equipped with Android OS 2.2)" we confirmed.

- 1) First, through the methods described in [i], the smartphone user is guided to an entrance site to the Website that performs one-click billing fraud (Figure 1-2).



Figure1-2: Entrance to the Website that Performs One-click Billing Fraud

- 2) If the user tries to access any of the video contents in 1), an Age-Verification Screen is displayed (Figure 1-3).
- 3) If the user pushes the "Aged 18 or over" button in 2), the use is prompted to download "Playback-Only Application" (Figure 1-4). But in fact, what is downloaded here is not a playback-only application but a virus spoofing as such application.
- 4) If the user pushes the "Download Playback-Only Application" button in 3), a file for that application (i.e., virus) is downloaded. If the user touches the file, another screen is displayed, indicating that the installation has been blocked (Figure 1-5). Note that this screen appears only if the smartphone is configured not to install "applications from unknown sources".



Figure 1-3: Age-Verification Screen



Figure 1-4: Confirmation Screen for Application Download

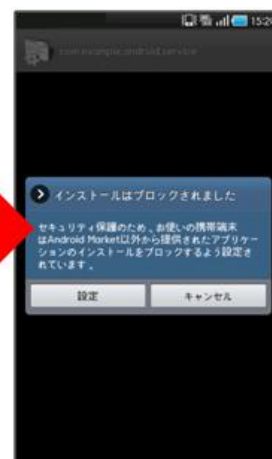


Figure 1-5: A Screen Indicating that the Installation of the Application Has Been Blocked

- 5) If the user pushes the "Settings" button in 4) to relieve the installation block, the "Change Settings" screen is displayed (Figure 1-6). At the time of purchase, the item "Permits the installation of applications from unknown sources (NB: this message is for Japanese Version)" is not ticked.
- 6) The user follows the steps of "How to install this application". Back to 5), the user ticks the item "Permits the installation of applications from unknown sources" (Figure 1-7).
- 7) If the user pushes the "Back" button on his/her smartphone and touches the downloaded application file, the "Installation Confirmation" screen is displayed (Figure 1-8).



Figure 1-6:
"Change Settings"
Screen (Type One)



Figure 1-7:
"Change Settings"
Screen (Type Two)

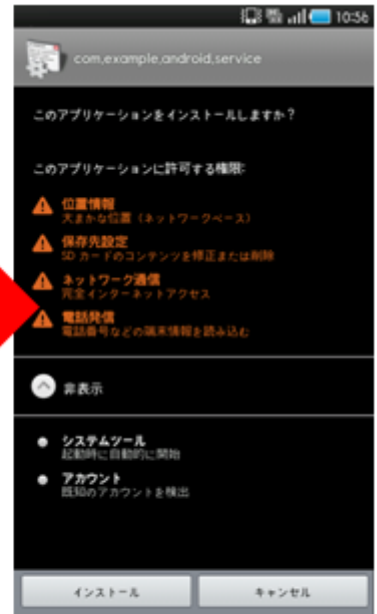


Figure 1-8:
Installation Confirmation
Screen

If we take a closer look at each item of "Permissions" in Figure 1-8, we see some unsuitable items deemed unnecessary for playback-only applications for the videos (i.e., outgoing-call, etc) (Figure 1-9). Note that the text and number of displayed items vary depending on the model and the timing of the website access.

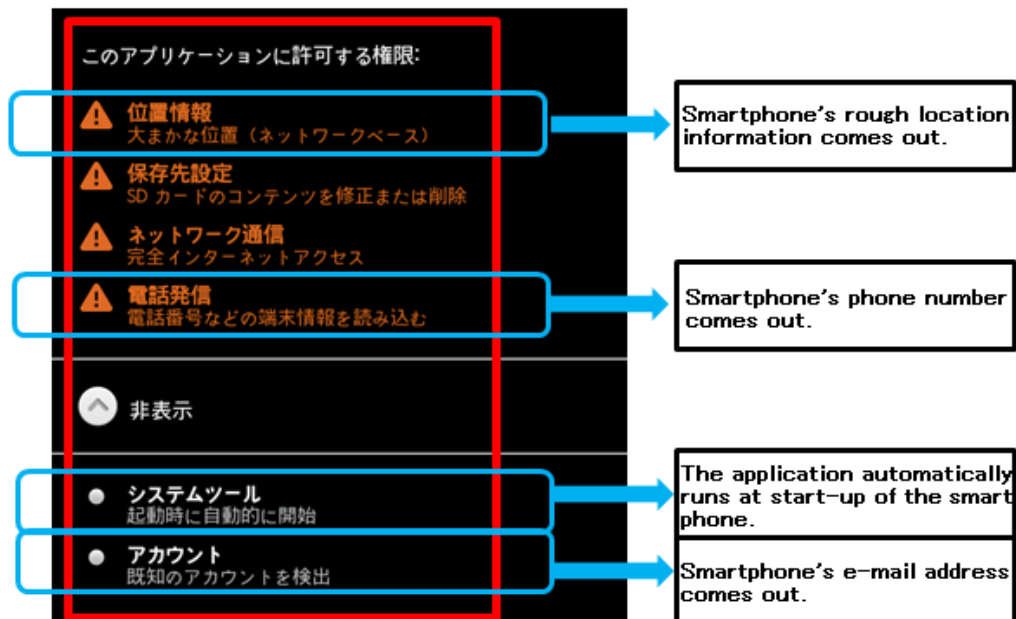


Figure1-9: Display Example of "Permissions"

- 8) If the user pushes the "Install" button in 7), the application is installed and the "Installation Completion" screen is displayed (Figure 1-10). That is to say, the installation of the virus has been completed.
- 9) If the user pushes the "Open" button in 8), a billing screen is displayed (Figure 1-11). Even if the user closes the browser, this billing screen reappears after a while. And even if the user pushes the "Exit" button in 8), this billing screen reappears after a while.
- 10) If the user pushes the "OK" button in 9) and rolls down the screen, the user sees the virus-infected smartphone's phone number and e-mail address displayed (Figure 1-12). This information is passed on to the one-click billing fraud operator as well.



Figure 1-10:
Installation Completion
Screen

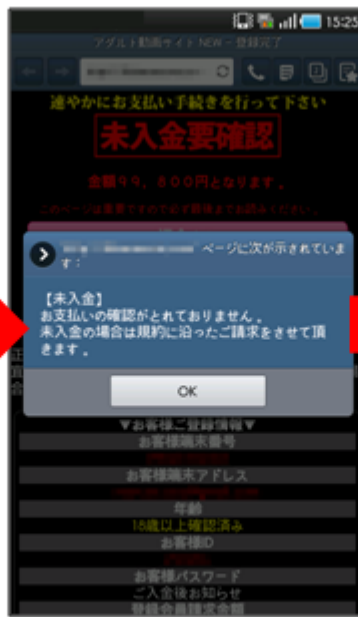


Figure 1-11:
Billing Screen (Type One)



Figure 1-12:
Billing Screen (Type Two)

- 11) In the smartphone's application list screen, the icon for the installed virus application is added (Figure 1-13).



Figure1-13: Display Example of the Added Application's Icon

- 12) For the smartphone that IPA examined this time, a payment-pressing SMS message was

sent from the operator at a later date (Figure 1-14). Since SMS is a service for sending messages to a cell-phone with the specified phone number, it is obvious that the smartphone's phone number was known to the operator. In such case, in order not to receive SMS messages from the operator, the user has to use the SMS rejection setting feature or change his/her phone number.



Figure1-14: Example of a Payment-Pressing SMS Message

The website that IPA confirmed this time was replaced, several days after the confirmation, with a website that does not leverage a virus. It is **thought that the one-click billing fraud operator (targeting smartphone) became wary as a one-click billing fraud operator targeting PCs had been arrested for "Unauthorized Creation of Electromagnetic Records" in January 2012.**

A Website which uses a similar technique might emerge in the future, so, by referring to "How to Avoid Being Infected with this Type of Virus", implement necessary measures on a regular basis.

(2) How to Avoid Being Infected with this Type of Virus

To avoid being infected with this type of virus, **as with PCs, it is important not to carelessly install any files downloaded from unreliable sites.** Countermeasures below are also effective.

[I] **Install security applications**

By installing a security application in your smartphone and keeping it up-to-date, you may be able to prevent the infection of this type of virus.

[II] **Configure your smartphone not to install applications from unreliable sites**

For applications to be used on smartphone, install them from a reliable site that performs application screening and removes malicious applications (e.g., Google's "Android Market" for Android devices). For this, configure your smartphone not to install "applications from unknown sources" and use it. If you need to install any applications from unknown sources, you may deactivate this setting once and install such applications, but be sure to activate this setting again after the installation.

[III] **Before you install any application, check for access permission**

Be sure to look through the list of "Permissions" that is displayed prior to the installation of an application and if you notice any unsuitable/suspicious items, do not install that application (Figure 1-15).

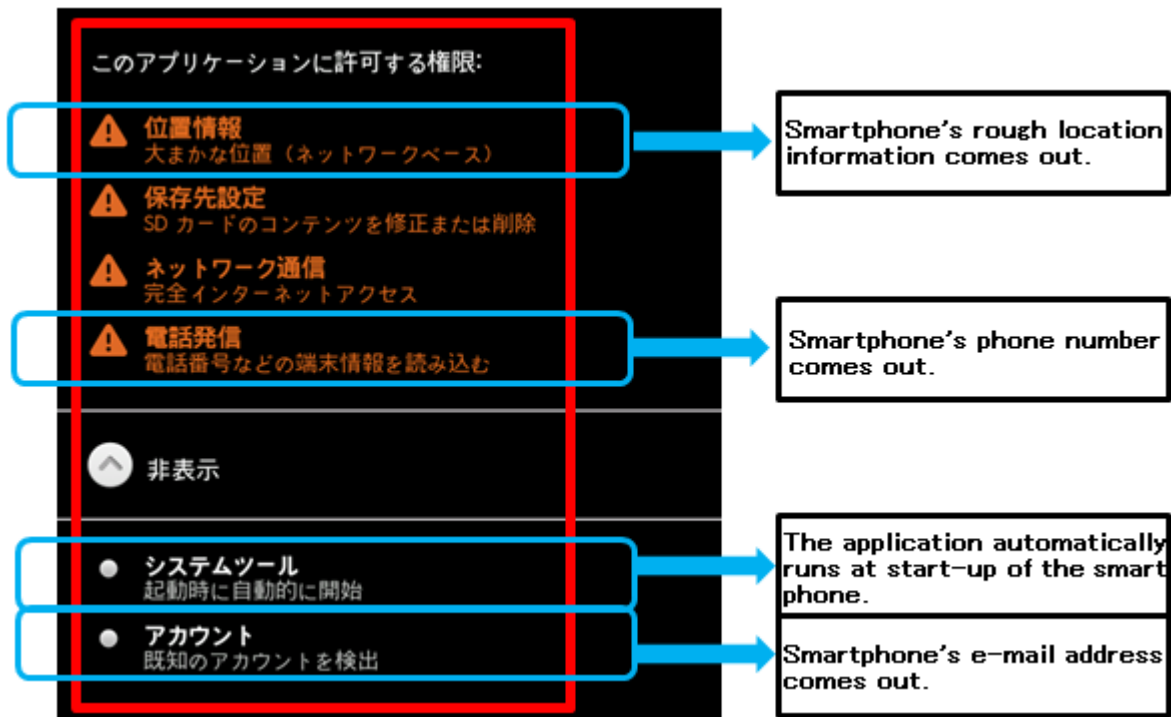


Figure1-13: Display Example of "Permissions"

(3) Should your smartphone be infected with this type of virus

Should your smartphone be infected with this type of virus, **by removing the installed application, you can prevent such billing screen from reappearing.**

How to remove applications varies depending on the Android OS version or the model. For details, contact your carrier, a cell-phone outlet, etc.

But because your smartphone's phone number and e-mail address are known to the one-click billing fraud operator, the operator might contact you by e-mail or phone. **If you receive a phone call or an e-mail from the operator, do not hold a conversation with them or e-mail them back. And should you receive such phone call or e-mail relentlessly, it is recommended to consult a local consumer affairs bureau or police.**

<Reference>

The nation's consumer affairs bureaus (National Consumer Affairs Center of Japan)

<http://www.kokusen.go.jp/map/> (in Japanese)

Reminder of the August 2011 issue, "Let's use your smart phone in a secure manner!" (IPA)

<http://www.ipa.go.jp/security/txt/2011/08outline.html> (in Japanese)

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

(1) Computer Virus Reported

While the virus detection count ^{*1} in January 2012 was **28,459**, up 114.6 percent from 13,259 in December 2011, the virus report count ^{*2} in January 2012 was **941**, up 23.2 percent from the December 2011 level (764).

*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 January, the virus report count, which was obtained by consolidating 28,459 virus detection reports, was 941.

W32/ Downad marked the highest detection count at **10,812**, followed by **W32/ Netsky** at **10,467** and **W32/ Mydoom** at about **5,158**.

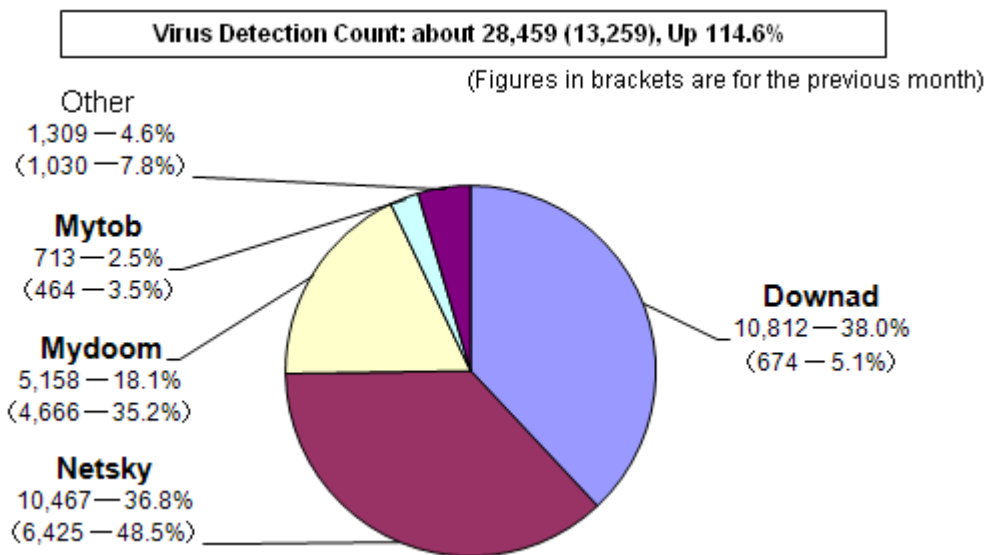


Figure 2-1: Virus Detection Count

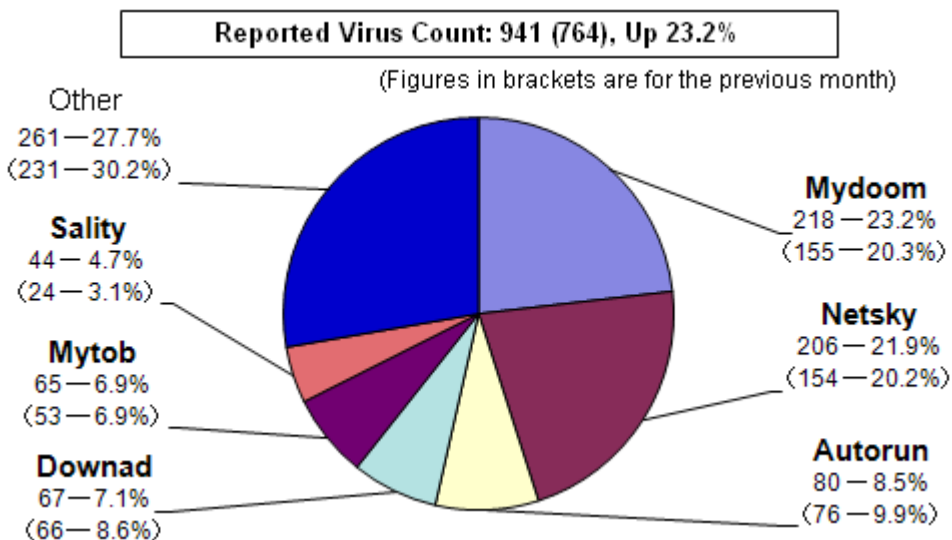


Figure 2-2: Virus Report Count

(2) Malicious Programs Detected

In January, BANCOS, which is a malicious program that steals IDs/passwords for online banking, was detected in great number (See Figure 2-3). And for RLTRAP, which showed a significant increase in September 2011, the detection count dropped to 7 in January.

* "Malicious Program Detection Count" here refers to the summary count of malicious programs that were reported to IPA in that month and that do not fall in the category of computer viruses defined by the "Computer Virus Countermeasures Standard".

* Computer Virus Countermeasures Standard (Announcement No.952 by the Ministry of International Trade and Industry): final decision was made on Dec. 28, 2000 by the Ministry of International Trade and Industry (MITI), which was renamed the Ministry of Economy, Trade and Industry (METI) on Jan. 6, 2001.

"Computer Virus Countermeasures Standard" (METI)

<http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm> (in Japanese)

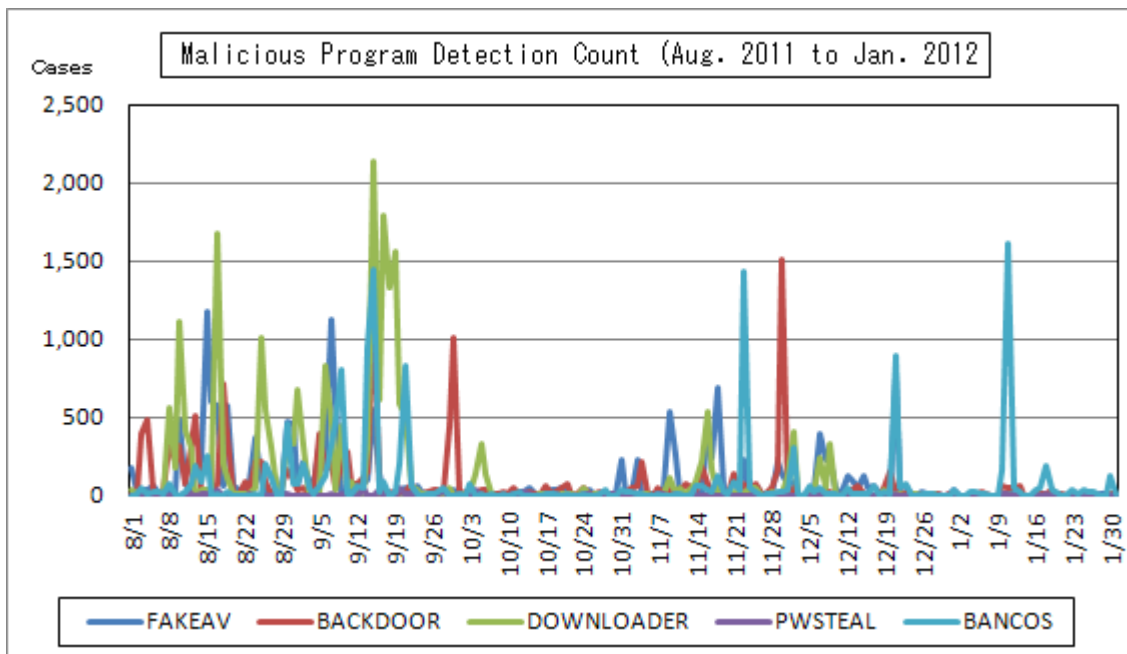


Figure 2-3: Malicious Program Detection Count

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

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

	Aug. '11	Sep.	Oct.	Nov.	Dec.	Jan. '12
Total for Reported ^(a)	10	7	15	7	7	8
Damaged ^(b)	8	5	8	5	7	7
Not Damaged ^(c)	2	2	7	2	0	1
Total for Consultation ^(d)	37	31	46	69	42	35
Damaged ^(e)	13	8	7	14	13	9
Not Damaged ^(f)	24	23	39	55	29	26
Grand Total ^(a + d)	47	38	61	76	49	43
Damaged ^(b + e)	21	13	15	19	20	16
Not Damaged ^(c + f)	26	25	46	57	29	27

(1) Unauthorized Computer Access Reported

The report count for unauthorized computer access in January was 8, 7 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 35. 9 of them reportedly had certain damages.

(3) Damages Caused

The breakdown of the damage reports were: **Spoofing (4); Intrusion (2); Unauthorized Mail Relay (1).**

Damages caused by "Spoofing" were: due to improper mail account management, an account was exploited to send spam e-mails (2); an online service being logged in by someone who successfully impersonated a legitimate user and used in an unauthorized manner (1); and so on.

Damages caused by "intrusion" were: a contents management tool was exploited to deface Web pages (1); data being stolen through the exploitation of improper PHP settings (1). The causes of "intrusion" were: a weak password being set (1); improper PHP settings (1).

(4) Damage Instance

[Intrusion]

(i) Our mail server was used as a stepping-stone for sending spam e-mails and got blacklisted

Instance	<ul style="list-style-type: none">- I found a great number of errors occurring on the internal mail server in our school, which was caused by a large accumulation of unsent e-mails.- Through the investigation, I found that the server was being used as a stepping-stone for sending spam e-mails, and that a massive amounts of spam e-mails were sent from a student's e-mail address. In the aftermath, the sending server of our school got blacklisted once, causing e-mails sent to some addresses to be rejected. This affected some staff's business operation.- Leakage of the student's password is thought to be the cause of this incident. We reminded all of our students to use a difficult password and place strict controls on their passwords.
----------	---

[Intrusion]

(ii) An account information is leaked and our web contents were interpolated

Instance	<ul style="list-style-type: none">- I received a phone call, saying "your company's Website is defaced".- Upon checking them, I found that our site had been altered so that the site visitors are forcibly taken to another website (which appears to be of a hacker group in China).- The login password for logging into Tomcat's management screen was easy-to-guess, so it is likely that the attacker cracked it and broke into the system.
----------	---

IV. Virus and Unauthorized Computer Access related Consultations

The total number of consultations in January 2012 was **1,302** **338** of which were related to "One-click Billing Fraud" (compared to 333 in December 2011); **18** to "Fake Security Software" (compared to 8 in December 2011); **11** to "Winny" (compared to 7 in December 2011); **4** to "A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data" (compared to 6 in December 2011)

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

	Aug. '11	Sep.	Oct.	Nov.	Dec.	Jan. '12
Total	1,651	1,551	1,496	1,420	1,312	1,302
Automatic Response System	958	936	865	746	790	760
Telephone	639	554	564	561	451	485
e-mail	50	52	55	102	65	49
Fax, Others	4	9	12	11	6	8

* 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)".

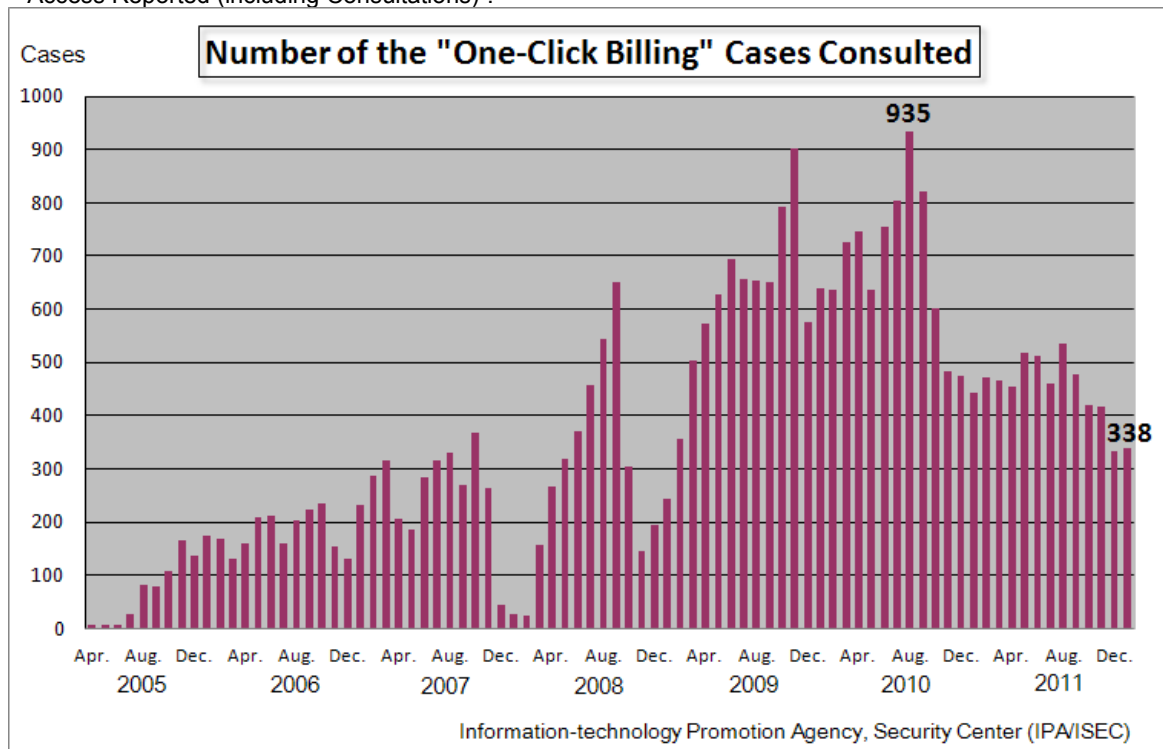


Figure 4-1: Number of the "One-click Billing Fraud" Cases Consulted

Major consultation instances are as follows:

(i) **In mistake for IPA, I asked another organization for help to solve the problem of one-click billing fraud**

<p>What was consulted</p>	<p>A billing screen for a sexually explicit site was pasted to my PC's screen and it does not disappear.</p> <p>When I consulted a consumer affairs bureau, I was advised to refer to IPA's website for the method to remove such billing screen. So I searched a search site by key words "IPA" and then clicked a URL that appeared at the top of the search result, taking it as IPA's.</p> <p>Although it was a paid service, I thought they would help me over the phone and followed their instruction, and was able to remove the billing screen. However, when I checked for the site I had accessed, it wasn't IPA's.</p> <p>I certainly searched IPA. What's going on?</p>
<p>Response</p>	<p>The organization you asked for help is not relevant to IPA.</p> <p>When you search a search site by key words, targeted information does not always appear at the top of the search result. Further, depending on the search site, advertisers' information may appear above the search result.</p> <p>When your search a search site for any information, be sure to carefully check for the title, URL and description so that you don't access wrong information. For IPA-provided information on one-click billing fraud, please refer to the webpage below.</p> <p><Reference> IPA - [Security Alert] Rapidly Increasing Cases Involving One-click Billing Fraud! The First Step for PC Users is to Learn its Mechanism! http://www.ipa.go.jp/security/topics/alert20080909.html (in Japanese)</p>

(ii) **Advertisements began to appear in the screen of my web browser,**

<p>What was consulted</p>	<p>Before I knew, advertisements began to appear in the lower right-hand corner of my web browser.</p> <p>Furthermore, an unknown toolbar was also displayed at the top of the web browser.</p> <p>I don't remember downloading anything to do with them. How can I remove them?</p>
----------------------------------	--

Response	<p>It is thought that an add-on (also called plug-in) for displaying advertisements has been embedded into your web browser.</p> <p>In the case of Internet Explorer, you can check for the add-ons currently embedded into the browser by selecting [Tool], [Add-on management]. By "disabling" or "removing" the corresponding add-on, you may be able to solve the problem. When you perform "disabling" or "removing", care should be taken so as not to "disable" or "remove" any necessary add-ons by mistake. If there is anything that is unclear, it is recommended to consult your PC's manufacture or the shop where you bought that PC. When you install an application or an add-on, another add-on might also be installed. So, be sure to carefully check for the messages on the confirmation screen that is displayed prior to the installation, and then avoid installing nonessential.</p> <p>Note that some add-ons such as "Adobe Flash Player" are pre-installed on most browsers and if such add-ons are obsolete in terms of version, only by visiting a malicious Website, your PC might be infected with a virus that exploits vulnerabilities in the add-ons.</p> <p>To eliminate PCs' vulnerabilities, it is important to update the application software installed, but updating add-ons tends to be forgotten. Be sure to update the add-ons on your PC.</p> <p><Reference> MyJVN Version Checker http://jvndb.jvn.jp/apis/myjvn/</p>
-----------------	--

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

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/201201/documents/virus1201.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/201201/documents/crack1201.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/>

Kaspersky : <http://www.viruslistjp.com/analysis/> (in Japanese)

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