



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Computer Virus/Unauthorized Computer Access Incident Report
- May 2010 -

This is the summary of computer virus/unauthorized computer access incident report for May 2010, compiled by Information-technology Promotion Agency, Japan (IPA).

I. Reminder for this Month

"Serious Damages Caused by False Antivirus Software"

In recent months, the number of consulted cases involving "False Antivirus Software (FAS)" type virus has been increasing, which was addressed several times in the "Reminder" column in the past. (See Figure 1-1) Recent trend of consultations concerning FAS-type virus is that, users of infected PCs experience more serious symptoms than ever before, including not being able to perform operation for system recovery. Moreover, in many cases, "Gumblar" (*1) is suspected to be the cause/route of infections. So if the PC was not secured enough with adequate security countermeasures, it might be infected with such virus by visiting a defaced Website.

A measure to prevent damages caused by FAS-type virus is, as with other viruses, to implement basic security countermeasures without omission. In this section, we present example of actual damages caused by this virus as well as countermeasures.

(*1) Gumblar: Refer to "Let's Learn the Mechanism of Gumblar and Take Appropriate Countermeasures" (the February 2010 issue by IPA)

<http://www.ipa.go.jp/security/txt/2010/02outline.html#5> (Japanese)

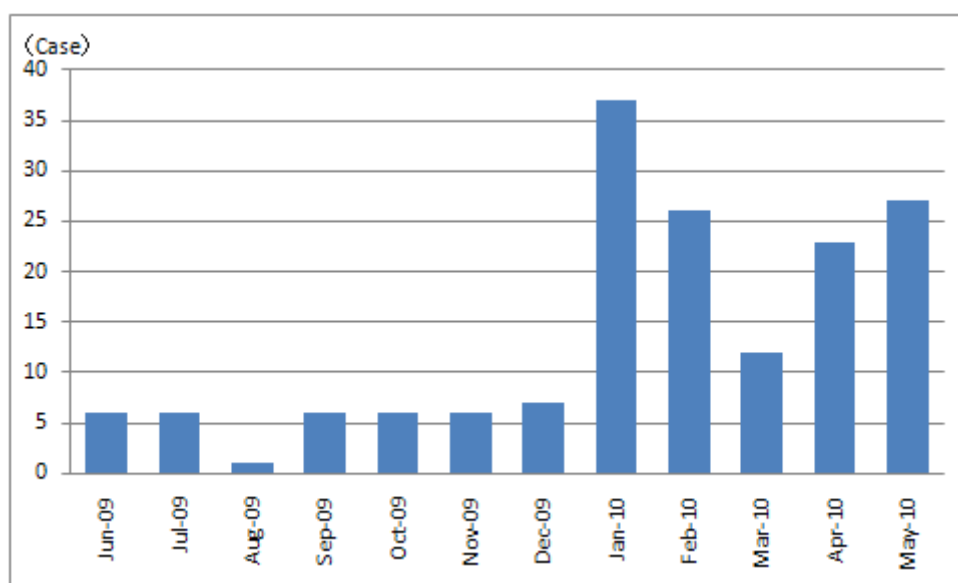


Figure 1-1: Number of consultations on FAS-type virus for one-year period

(1) Overview of FAS-Type Virus

FAS-type virus is a fraudulent virus that displays a falsified warning message (e.g., "YOUR SYSTEM IS INFECTED WITH A VIRUS", "YOU NEED TO BUY A SOFTWARE PRODUCT TO SOLVE THIS PROBLEM") and urges the PC's user to e.g., supply his credit card number to bilk him out of money. It displays authentic-looking screens that are hardly distinguishable from those of legitimate antivirus software as well as software name that sound authentic such as "Security essentials 2010" and "XP Smart Security 2010" (many other names have been confirmed to be used for FAS). So, cautions should be exercised.

Some of FAS-type viruses are designed to impede virus-cleaning or data backup from the PC, which may result in serious damages. For more information on FAS-type virus, refer to the Reminder section in the November 2009 issue.

<Reference>

"Threat of False Antivirus Software is Growing Again" (Reminder in the November 2009 issue by IPA)

http://www.ipa.go.jp/security/english/virus/press/200910/E_PR200910.html

(2) Example of Actual Damages

In this section, we present specific examples of consulted/reported cases. Figure 1-2 shows (part of) a screen shot of FAS-type virus with which the consulter infected in the case example below.

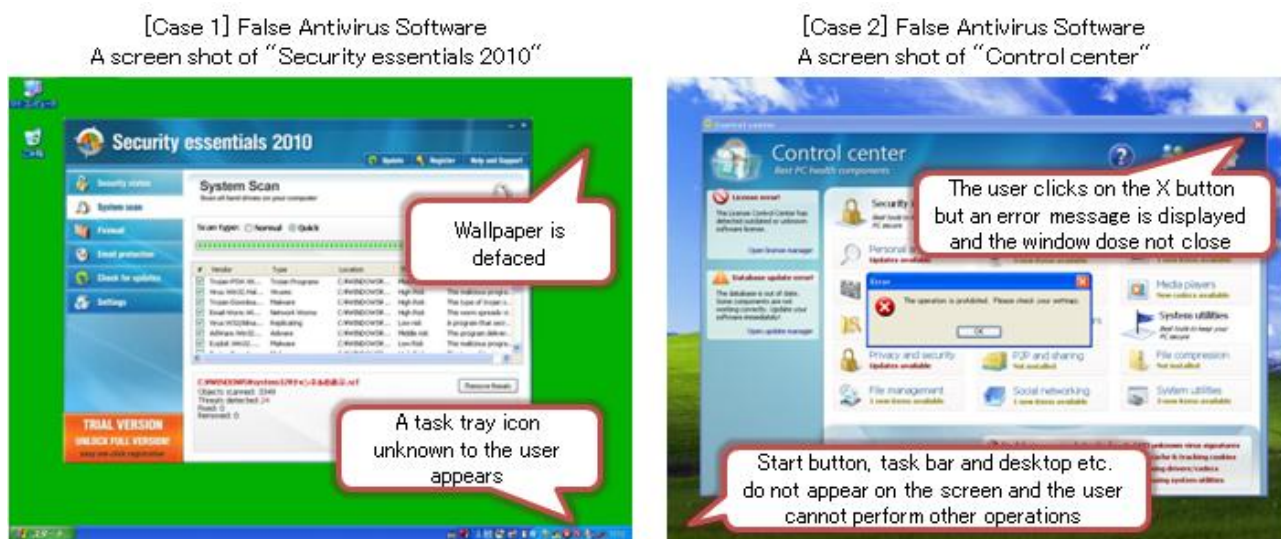


Figure 1-2: Example of Screens Shots of FAS-Type Virus Infection

[Case 1]

<p>What was consulted</p>	<p>When I was browsing a Japanese Website, the site was suddenly replaced by an English Website and it did not disappear even after I rebooted my PC. A message "YOUR SYSTEM IS INFECTED" is shown on the screen. Though I started my PC in "Safe Mode" (*2), the warning message in English was still on the screen. I was unable to activate "Task Manager" (*3) and/or "System Restore" (*4) and to use my PC as normal.</p>
<p>Software Name</p>	<p>Security essentials 2010</p>
<p>Commentary</p>	<p>"Security essentials 2010", which the consulter's PC was infect with, is a virus for which consultations were made frequently in May. It has nothing to do with "Microsoft Security Essentials" which is antivirus software provided by Microsoft. Apparently, such confusing name is used to mislead users into thinking that it is useful software. For this virus, the consultations have been made to IPA since February of this year.</p>

(*2) Safe Mode: A specific way to start Windows, which is used e.g., to perform recovery operations on a PC.

(*3) Task Manager: A tool used to display the list of programs running on a PC, from which users can abort programs.

(*4) System Restore: A tool that comes with Windows and is used to restore the previous settings of a PC.

[Case 2]

<p>What was consulted</p>	<p>When I started my PC, a window was displayed, indicating that my license for the antivirus software had expired and urging me to pay a licensing fee. So I started my PC in "Safe Mode" but I had the same situation and was unable to perform further operations. Because necessary information was stored in that PC, I could not initialize it, so I entered my credit card number. Then the PC become operable but the files on the desktop disappeared.</p>
<p>Software Name</p>	<p>Control center (Control center - Best PC health components)</p>
<p>Commentary</p>	<p>This is the case where not only were PC and its data damaged but also financial loss was incurred. Intention of the virus creator is to have the PC user pay a licensing fee by rendering the infected-PC inoperable. Infection route in this case is still unknown, but the consulter reportedly opened an email to which a suspicions file was attached just before the infection. In such cases, there is no guarantee that the situation would improve by purchasing licenses, so you should not pay for it</p>

[Case 3]

<p>What was consulted</p>	<p>When I was using the Internet, a large volume of messages in English appeared on the screen and the PC stopped functioning properly. When I contacted the PC's manufacture, I was instructed to perform initialization, so I did it. It was "Security Tool" that my PC had been infected with. Was my response correct?</p>
<p>Software Name</p>	<p>Security Tool</p>
<p>Commentary</p>	<p>Security Tool is a virus which turns the color of the screen into ice-blue. For this virus, consultations have been made to IPA since the end of 2009. Initializing the infected PC was a correct response. However, the problem lies in the fact that the consulter contracted that virus as he was browsing a Website by using a PC not secured enough. If the consulter himself was unable to implement adequate security countermeasures, he might suffer the same damage.</p>

Apart from the above-mentioned FAS-type viruses, the following FAS-type viruses were consulted/reported to IPA in May. It can be thought that various types of viruses have been spread in widely-scattered areas.

- XP AntiMalware 2010
- XP Smart Security 2010
- Live Security Suite
- Data Protection
- Digital Protection
- Desktop Security 2010

If you experience symptoms similar to those of the case examples above or see virus scan screen that you haven't seen before (as in Figure 1-2), it is highly likely that your PC is infected with FAS-type virus. At the same time, viruses other than FAS-type virus might have penetrated into your PC. To recover from this kind of situation, please follow the steps in (3).

For protective measures to prevent damages caused by FAS-type virus, refer to (4).

(3) How to Respond in the Event of Infection

As shown in the case examples, once infected with FAS-type virus, it might be difficult to restore the systems or clean the virus. By referring to the following guideline to respond to the virus infection, try to improve symptoms and/or recover the systems.

- If the PC is operable, scan it by using the latest antivirus software and try to clean the virus.
 - If you don't have antivirus software, you can use "online scan" provided by antivirus software vendors on their Websites.
- If you cannot clean the virus by using the antivirus software, try to recover your systems by performing "System Restore" (See (iii)).
- If the PC is not operable or the virus was not cleaned by the antivirus software, or "System Restore" was not properly performed, start the PC in "Safe Mode" (See (ii)) and re-try the above-mentioned steps:

- If you cannot even shutdown your PC, press the main unit's power button for a while (i.e., forcibly turning the power off) and start the PC in "Safe Mode."
- If the systems have not been recovered by following the above-mentioned steps, perform initialization (a process of restoring factory default settings) on that PC. For a PC infected with FAS-type virus, users might be able to perform operations to some degree, but it is risky to continue to use that PC as it may result in information leakage incurred by the virus.

Cautions and steps that should be followed in implementing countermeasures are as follows:

(i) Do not pay the licensing fee for FAS

There is no guarantee that the situation would improve by paying the licensing fee (See case 2). If you entered your credit card number, that information might also be abused. You should be careful not to pay for such fees as it may help activities of a person with malicious intent.

(ii) Use "Safe Mode"

By starting Windows in "Safe Mode", you might be able to limit the movement of that virus and to use a tool that did not work properly in normal mode due to the interference by that virus. Using the "Safe Mode, try **data backup, virus-cleaning by antivirus software, or "System Restore"**, etc.

For information on how to use "Safe Mode," refer to the Websites below. Ways to start PCs in "Safe Mode" may vary depending on their models, so if you have any questions, please contact your PC's manufacture.

<Reference>

To start the computer in safe mode (windows xp)(Microsoft)

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/boot_fa1safe.msp?mfr=true

Start your computer in safe mode (windows vista)(Microsoft)

<http://windows.microsoft.com/en-us/windows-vista/Start-your-computer-in-safe-mode>

To start the computer in safe mode (windows 7)(Microsoft)

<http://windows.microsoft.com/en-us/windows7/Start-your-computer-in-safe-mode>

(iii) Recover the systems by "System Restore"

If you are using the latest antivirus software and if the symptom does not subside, you might be able to improve the situation by performing "System Restore." "System Restore" is a tool that comes with Windows XP, Windows Vista and Windows 7 and is used to restore the previous state when there is any problem in using the PC (e.g., PC behaving in an erratic way.)

<Reference>

Windows XP System Restore Is Easy to Use(Microsoft)

http://www.microsoft.com/windowsxp/using/helpandsupport/getstarted/ballew_03may19.mspx

What is System Restore? (windows vista)(Microsoft)

<http://windows.microsoft.com/en-us/windows-vista/What-is-System-Restore>

Windows 7 features "System Restore"(Microsoft)

<http://windows.microsoft.com/en-us/windows7/products/features/system-restore>

Specific steps to start Windows in "Safe Mode" and perform "System Restore" are presented in the following Website:

<Reference>

"Procedure to Perform 'System Restore' on Windows" (IPA)

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

(iv) **Initialize PC**

If the symptom does not subside, perform initialization.

In the case of FAS-type virus, the infected PC might be infected with several other viruses and even when it seems that the PC has been restored, the possibility of some viruses remaining in the PC cannot be ruled out. To clean all the viruses, IPA recommends initialization as its principle. Especially, if your PC behaves in an erratic way or if you feel something unusual in using your PC, consider performing initialization.

When performing initialization, remember that all the data in that PC is deleted, so if the PC is operable as normal, we recommend backing up important data first. For procedures to initialize you PC, refer to the Sections such as "Restore factory default settings" in the PC's instruction manual.

Note that right after the initialization, the PC might not be secured enough with adequate security countermeasures. To avoid falling victim again, be sure to implement proactive measures in (4). And before restoring backup data into the initialized PC, perform virus check on it.

(4) **Proactive Measures**

If the PC is missing any of the required security countermeasures, there is a risk of suffering from the damages as described in the cases examples above while being connected to the Internet. As a safeguarded for not only FAS-type virus but also other viruses, implement the following basic countermeasures without omission:

(i) **Regularly perform data backup**

Remember that data stored in a PC might be lost anytime due to a computer virus or other causes (e.g., breakdown of the PC) and regularly back up important data. For FAS-type viruses, some are designed to impede data backup from PCs, so it might be too late to restore the most recent data after having a security incident.

(ii) **Install Antivirus Software**

Antivirus software is not all-round tool; however, installing such software is one of the important security countermeasures. By installing antivirus software and keeping virus definition files updated, you can block the penetration of computer viruses or clean the viruses that have already entered into your PC. Because many of recent viruses make it difficult for the victims to see if their PCs have been infected only by looking at the screen, it is indispensable to install antivirus software.

For general users, we recommend using "Integrated" antivirus software that has a feature to block the access to a suspicious Website along with a feature to detect and clean computer viruses.

(iii) Eliminate vulnerability

"Web Infection type virus", for which the user of a PC contract a computer virus only by visiting a Website and which is used in "Gumblar", exploits **vulnerability** in the PC that is "**a deficit that allows a computer virus to enter the PC.**" Therefore, eliminating vulnerability is one the important security countermeasures.

Vulnerability might exist in OS (such as Windows), Browser (such as Internet Explorer) and other applications software. For software products installed on your PC, we recommend that all of them be updated to the latest versions with existing vulnerabilities remedied.

Supplementary explanation on how to update software products are as follows:

- Updating Windows (OS itself), Internet Explorer and Microsoft Office (Word, Excel)
 - For some PCs, the "Automatic Update" function for these software products is enabled so that they are automatically updated to the latest ones. When manually updating these software products, use "Windows Update" or "Microsoft Update." For more information, refer to Microsoft's Web pages.
 - <Reference> Microsoft Update overview(Microsoft)
<http://www.microsoft.com/security/updates/mu.aspx>
- Confirming by "MyJVN Version Checker"
 - IPA provides a tool on its Website that allows users to check if Adobe Flash Player and other software products that often become the target of a computer virus are installed on their PCs and if such software products are the latest ones. For more information, refer to the Web page "MyJVN Version Checker" below. For information on how to use "MyJVN Version Checker" and to update software products to the latest ones, refer to the Webpage "To Prevent Virus Infection via a Web Page."
 - <Reference> "MyJVN Version Checker" (IPA)
<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK> (Japanese)
* As of June 2010, Windows XP and Vista are supported.
 - <Reference> "To Prevent Virus Infection via a Web Page" (CCC)
<https://www.ccc.go.jp/detail/web/index.html> (Japanese)
- Other software
 - Ways to update software products vary depending on the product. It is favorable for you to understand what software products are installed on your PC and to regularly update them. It might be difficult for novice PC users to implement it, but they should also learn the knowledge and operating manner to defend themselves.
- Collecting information on vulnerabilities
 - IPA issues a security alert when vulnerability was detected in a software product used by many general users. By periodically referring to the Webpage "Information on Emergency Countermeasures and A List of Security Alerts" below, check if a software product for which security alert was issued is installed on your PC, and then take appropriate countermeasures.

- <Reference> "Information on Emergency Countermeasures and A List of Security Alerts"
<http://www.ipa.go.jp/security/announce/alert.html> (Japanese)
- "From the time vulnerability is detected to the time a patch to correct the program (security patch) is released" there is a certain period in which the detected vulnerability cannot be remedied. An attack that targets this period is called "Zero-Day" attack, which is very difficult to defend. If this attack became prevalent, it would become risky to use the Internet.
In the case of "Zero-Day" attack, vulnerability cannot be remedied until a security patch is provided, so you need to respond to it by taking alternative countermeasures (i.e., workaround.) "Workarounds" vary depending on the software product (e.g., stopping a problematic feature by changing the software settings, removing the problematic software product from that PC so that it cannot be exploited, etc.)
The above-listed Web page "Information on Emergency Countermeasures and A List of Security Alerts" contains information on "Zero-Day" attack as well. Before implementing workarounds, you should check first for the information provided as the implementation might influence other features/functions.
- For more information on "Zero-Day" attack, refer to the Web page below.
<Reference> "About Zero-Day Attack That Exploited Vulnerability Before A Security Patch Was Provided" (IPA)
<http://www.ipa.go.jp/security/virus/zda.html> (Japanese)

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

(1) Computer Virus Reported

While the virus detection count ^(*) in May was about 50,000, up 26.8 percent from about 40,000 in April, the virus report count ^(**) in May was 1,084, equivalent level of 1,077 in April.

(*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 May, the virus report count, which was obtained by consolidating about 50,000 virus detection reports, was 1,084.

W32/Netsky marked the highest detection count at about 37,000, followed by **W32/Koobface** at about 7,000 and **W32/Mydoom** at about 4,000.

Virus Detection Count: about 50,000 (40,000), Up 26.8 percent

(Figures in brackets are for the previous month)

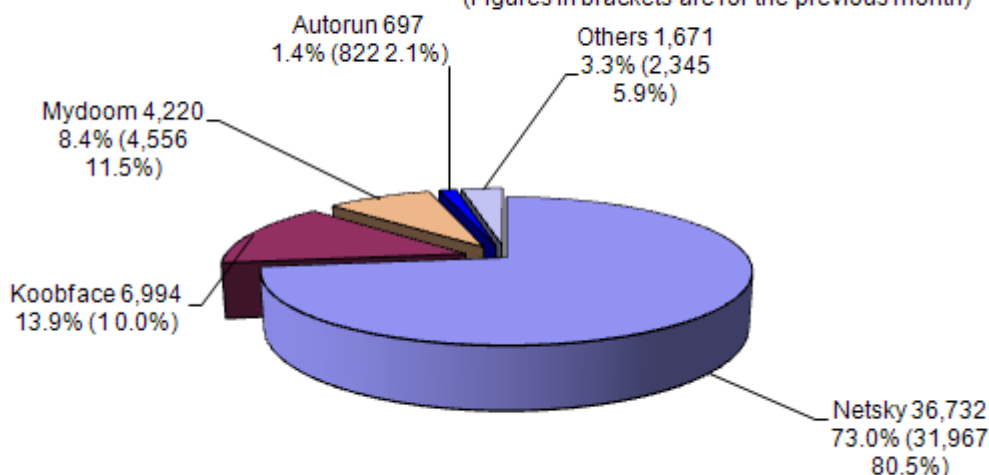


Figure 2-1: Virus Detection Count

Reported Virus Count: 1,084 (1,070), Up 0.6 percent

(Figures in brackets are for the previous month)

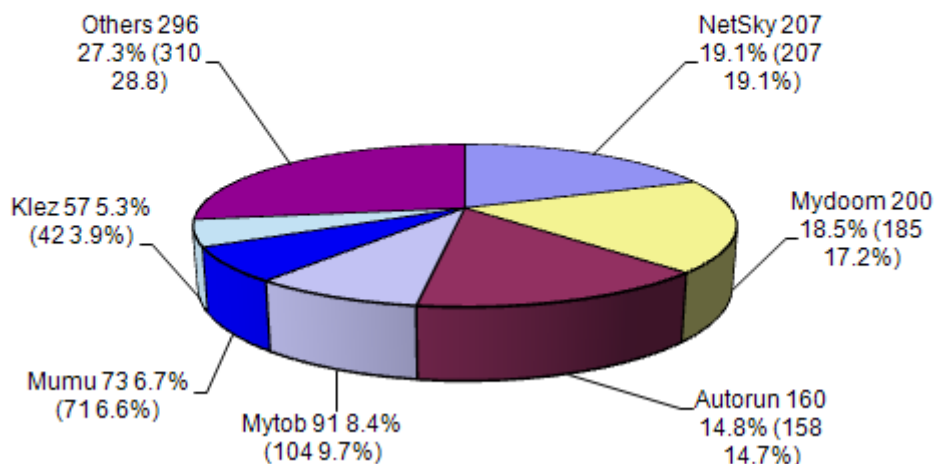


Figure 2-2: Virus Report Count

(2) Malicious Programs Detected

For the number of malicious programs detected, we have not seen a significant difference between April and May 2010. However, FAKEAV which is a FAS-type virus have been frequently detected in May. (See Figure 2-3)

Because most of malicious programs are contained in an e-mail attachment and distributed, you should be careful in handling an e-mail attachment. In some cases, attackers use Bot-infected PCs to distribute malicious programs.

Cyber Clean Center (CCC) provides anti-Bot measures as well as online Bot-removal tools. To avoid taking part in the e-mail distribution of malicious programs, check your PC for Bot infection, and then implement infection-prevention measures, including blocking the entry of malicious programs.

<Reference>

“Knowledge of How to Prevent Infection” (Cyber Clean Center)

<https://www.ccc.go.jp/knowledge/> (in Japanese)

* Cyber Clean Center is a Bot countermeasure project launched by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry.

<Reference> About Cyber Clean Center

<https://www.ccc.go.jp/ccc/> (in Japanese)

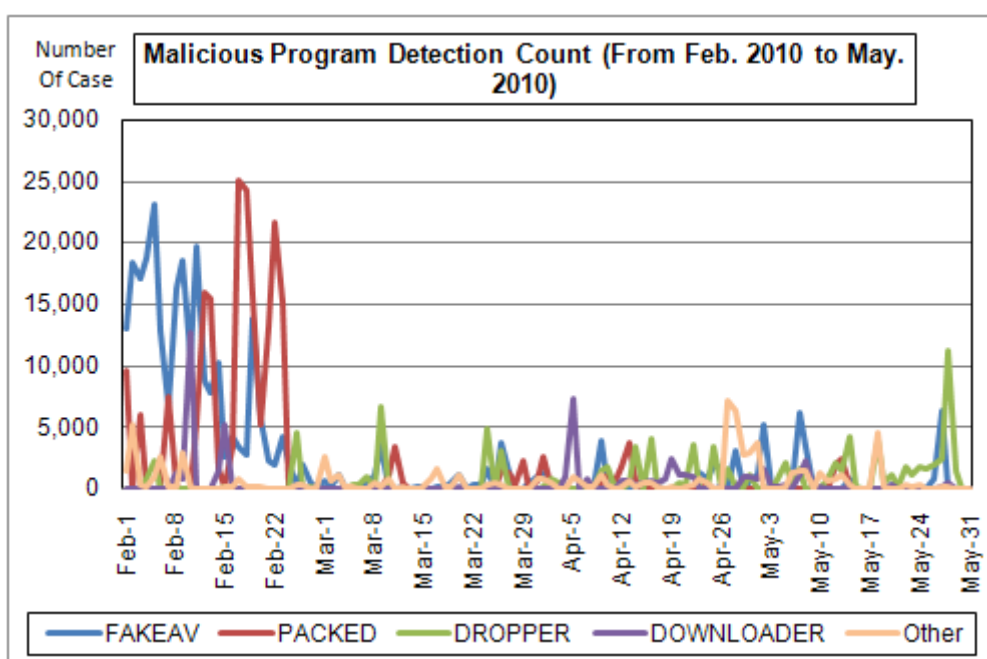


Figure 2-3: Malicious Program Detection Count

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

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

	Dec.	Jan. '10	Feb.	Mar.	Apr.	May
Total for Reported ^(a)	9	20	27	19	11	8
Damaged ^(b)	6	12	17	13	10	5
Not Damaged ^(c)	3	8	10	6	1	3
Total for Consultation ^(d)	22	67	47	60	39	52
Damaged ^(e)	14	34	28	23	16	22
Not Damaged ^(f)	8	33	19	37	23	30
Grand Total ^(a + d)	31	87	74	79	50	60
Damaged ^(b + e)	20	46	45	36	26	27
Not Damaged ^(c + f)	11	41	29	43	24	33

(1) Unauthorized Computer Access Reported

The report count for unauthorized computer access in May 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 52 (2 of which were also included in the report count). 22 of them reportedly had certain damages.

(3) Damages Caused

The breakdown of the damage reports were: **intrusion (3); spoofing (1); others (1).**

Damages caused by "intrusion" were: a Web page being defaced (2), with both cases involving malicious code embedded; malicious programs being embedded into a Web server, which in turn served as a stepping stone for attacking other sites (1). The cause of the intrusion has not been fully identified, but two cases was suspected to have been caused by "Gumblar"; one due to a poor ID/password management (password cracking attack* was thought to have been carried out against a port used by SSH*.)

Damages caused by "spoofing" included: online service (online game (1)) being used by someone who successfully impersonated a legitimate user and logged on.

* SSH (Secure Shell): a protocol that allows someone using one computer to communicate with a remote computer via the network.

* Password cracking: a process of finding out other person's password, e.g., through a password analysis. This includes Brute Force attack and Dictionary attack. There are also password-cracking programs.

(4) Damage Instance

[Intrusion]

(i) Damages Apparently to Have Been Caused by "Gumblar"

Instance	<ul style="list-style-type: none"> ● I was notified by a client who had accessed my company's Website that, "When I was viewing the Home page, a virus alert was displayed." ● When I inspected the Web contents, I found that a script to lead site visitors to a malicious site was embedded in a HTML source code. ● When I looked into access logs for an ftp used for updating Web contents, I found that a login attempt had successfully been made from an IP address unknown to me. The ftp account was only made available to company personnel, so the reason why the account information has been leaked is still unknown. ● As a countermeasure, I decided to place restrictions on IP addresses from which ftp connection can be made.
----------	---

[Spoofing]

(ii) Online Game Account Hijacked

Instance	<ul style="list-style-type: none"> ● I signed up a free game site. One day, when I tried to log onto the site, a message "Entered a wrong password" appeared and I was unable to log on to the site. ● When I contacted the company operating the game site, I was told that my password had been changed. I don't know how this happened. ● Based on the registered information, the game site operator confirmed that the owner of the account was me. But they say I need to pay 1,000 yen to have my password reissued.
----------	--

IV. Unauthorized Computer Access Consulted

The total number of consultations in May was 1,881. 637 of which were related to "One-Click Billing Fraud" (compared to 747 in April); 27 to "Hard Selling of Security Software" (compared to 23 in April); 5 to "Winny" (compared to 11 in April); 4 to "A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data" (compared to 4 in April).

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

	Dec.	Jan. '10	Feb.	Mar.	Apr.	May
Total	1,794	2,150	1,789	2,000	2,110	1,881
Automatic Response System	1,138	1,160	977	1,057	1,194	1,091
Telephone	602	910	736	846	835	714
e-mail	52	78	70	92	81	76
Fax, Others	2	2	6	5	0	0

* IPA provides consultation/advises for computer virus, unauthorized computer access, problems related to Winny as well as overall information security.

E-mail address: virus@ipa.go.jp (Virus); crack@ipa.go.jp (Unauthorized Computer Access); winny119@ipa.go.jp (Crisis-Line Phone Call for Problems Related to Winny); fushin110@ipa.go.jp (Suspicious E-Mail 119); isec-info@ipa.go.jp (Other Security Relevant Issues)

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)".

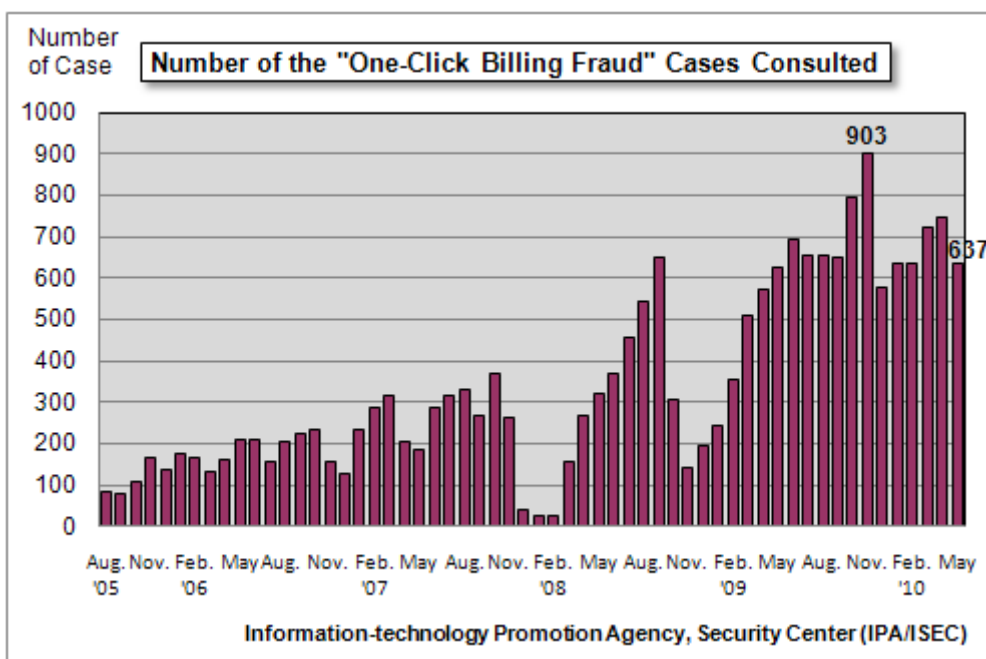


Figure 4-1: Number of the "One-Click Billing Fraud" Cases Consulted

Major consultation instances are as follows:

(i) I lent my PC to an acquaintance and the PC was returned with a billing message for an adult site displayed

<p>What was consulted</p>	<p>I lent my PC to an acquaintance for a couple of days and the PC was returned with a billing message for an adult site displayed. What should I do with this PC?</p>
<p>Response</p>	<p>Apparently, the person whom you lent your PC was accessing an adult site and despite security alert being displayed, he continued risky actions for which he contracted one-click billing fraud virus by himself. We recommend that you perform "System Restore" function to restore the PC's settings back to one day before lending it.</p> <p>In the case of consultation above, the PC was infected only with one-click billing fraud virus, but if the PC had been infected with other viruses that cause PC data to be leaked, it would have led to a catastrophic damage. Especially, if the PC handles information whose leakage brings you much trouble, you should not lend it to others.</p> <p><Reference> IPA – [Security Alert] Rapidly increasing consultations on "One-Click Billing Fraud" http://www.ipa.go.jp/security/topics/alert20080909.html (in Japanese)</p>

(ii) I want check whether or not my Website has been defaced

<p>What was consulted</p>	<p>I was pointed by a client, "Don't you think your company's Website has been defaced"?' Is there a simple way to check for Website defacement?</p>
----------------------------------	--

Response	<p>If you have a corresponding Web page file that you are certain about not being defaced, you can compare it with the latest Web page file to check for defacement. If such file is unavailable, copy all the page files on the Website to your PC and scan them for computer viruses by using a single or multiple (if possible) antivirus software with their pattern files updated. You can also use free online scan.</p> <p>If the Website has been defaced, a virus might be detected. On the other hand, even if no virus was detected, that Website might have been defaced. Remember that scanning is just a simplified way to detect such defacement. For more accurate comparison, you should write into CD or DVD the files that have been confirmed to be safe so they can be kept undefaced at your hand.</p> <p><Reference></p> <p>IPA – To Website Administrators: Security Alert about Website Defacement To General Users: Security Alert about Virus Infection Via A Defaced Website</p> <p>http://www.ipa.go.jp/security/topics/20091224.html (in Japanese)</p>
-----------------	---

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

According to the Internet Fixed-Point Monitoring System (TALOT2), **125,020** unwanted (one-sided) accesses were observed at ten monitoring points in May 2010 and the total number of sources* was **49,574**. This means on average, **403 accesses** form **160 sources** were observed at **one monitoring point per day**. (See Figure 5-1)

*Total number of sources: indicates how many accesses 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.

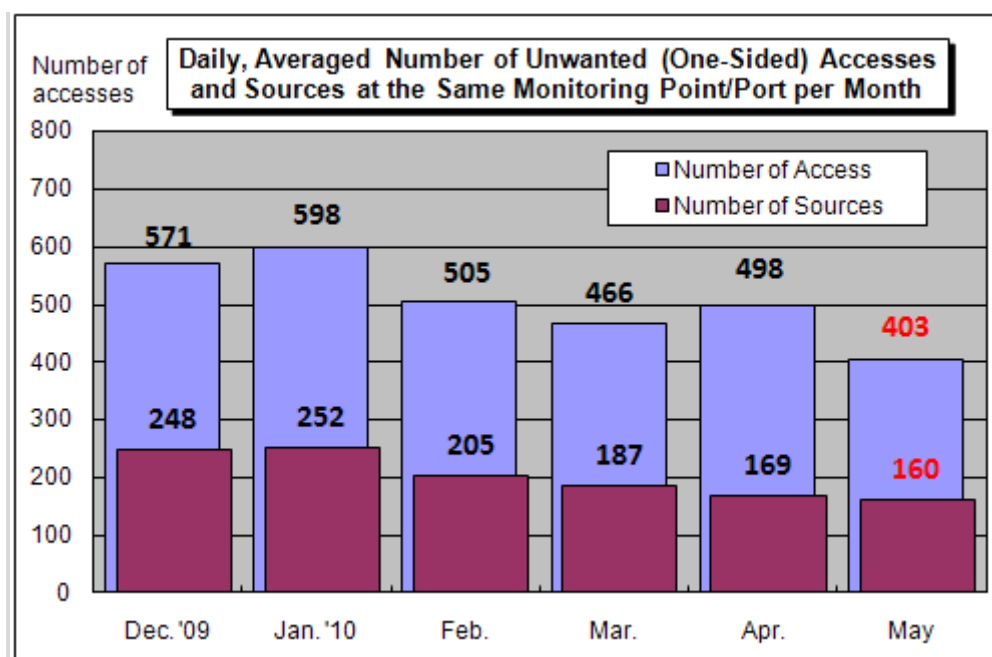


Figure 5-1: Daily, Averaged Number of Unwanted (One-Sided) Accesses and Sources at the Same Monitoring Point/Port per Month

The Figure 5-1 shows daily, averaged number of unwanted (one-sided) accesses and sources at the same monitoring point/port per month (from December 2009 to May 2010). As shown in this Figure, the number of unwanted (one-sided) accesses decreased in May compared to April.

The Figure 5-2 shows the May-over- April comparison results for the number of unwanted (one-sided) accesses, classified by destination (port type). As shown in this Figure, access to 9415/tcp and 21329/tcp, which wasn't ranked high in the past, has been ranked high in May. It has yet to be identified why these ports were accessed as they are not the ones used by a specific application.

As for 9415/tcp, access from multiple sources in overseas (mainly China) observed at multiple monitoring points of TALOT2 has been on the rise since March. (See Figure 5-3) Similar increasing trends have also been observed by other organizations undertaking fixed point observations, indicating that such access was made in widely-scattered areas, so we need to pay attention to observations status on an ongoing basis.

As for 21329/tcp, access from a single source in the U.S observed at a single monitoring point of TALOT2 have increased rapidly in May.

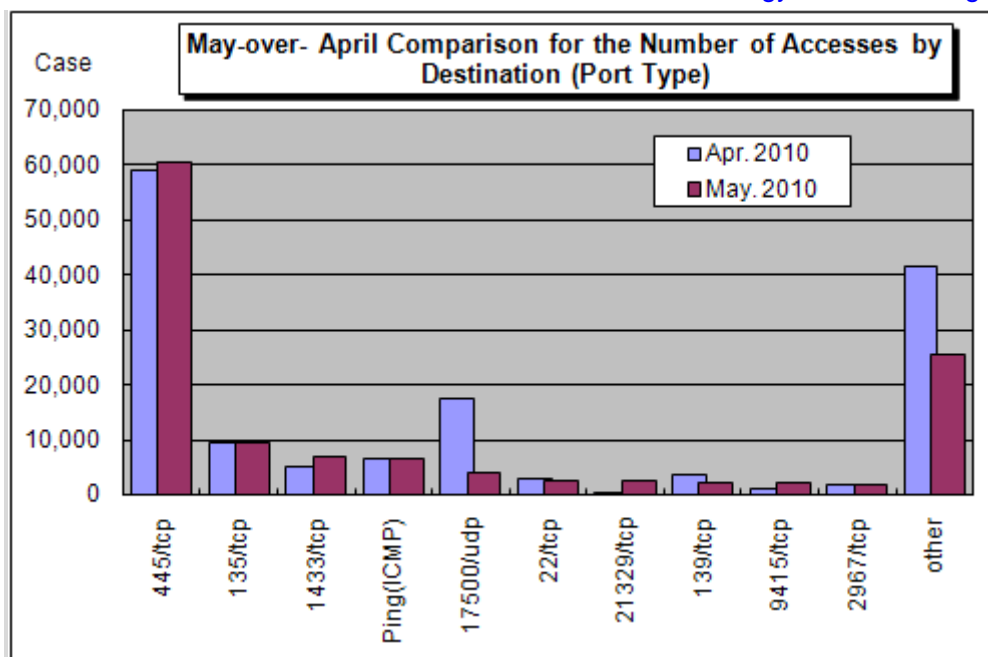


Figure 5-2: May-over- April Comparison for the Number of Accesses by Destination (Port Type)

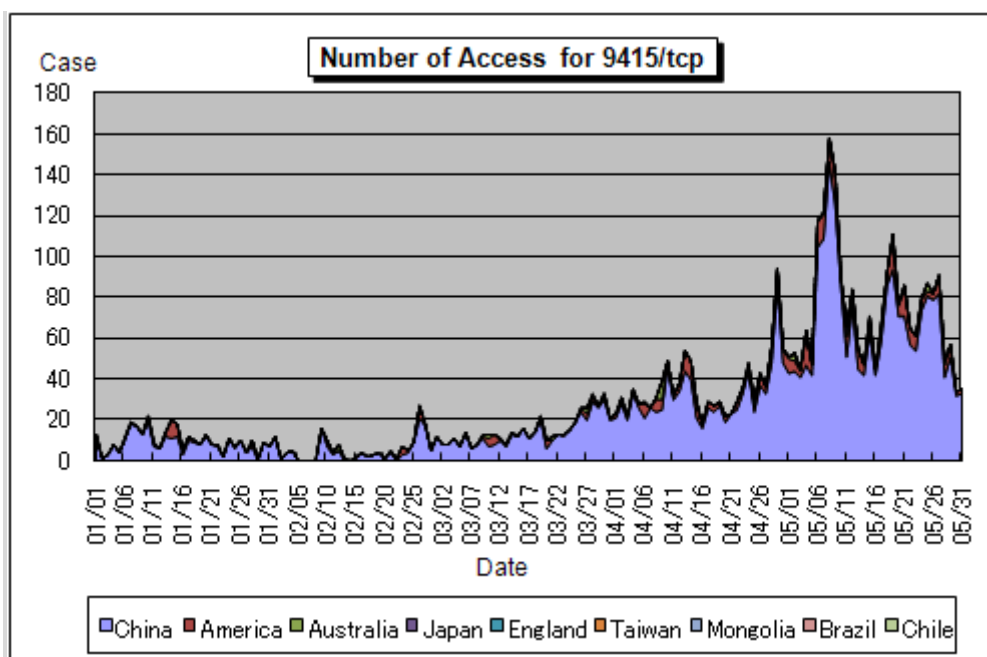


Figure 5-3: Number of Access for 9415/tcp

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/201005/documentsTALOT2-1005.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)

Hanamura/Kagaya/Ooura

Tel.: +81-3-5978-7527

Fax: +81-3-5978-7518

E-mail: isec-info@jpa.go.jp