

***Computer Virus/Unauthorized Computer Access
Incident Report - May 2009***

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

I. Reminder for the Month

**“Be Cautious with the Computer Virus which Masquerading to be the Alert for H1N1 FLU Virus!”
- Be sure to check the authenticity of that alert -**

As everyone is aware that the new flu virus, “H1N1” has been spreading all over the world from the end of April: the virus masquerading to be the alert relevant to the new “H1N1” flu virus that “me-too” infects computer is also enlarged. Of the consultations rushed to IPA, there identified several cases that some malicious intents attempted computer to infect (computer) virus by appending it to fictitious alert masquerading to be the one of actual research institutions.

As with the case, immediately after the news reports globally watched and the rightly before the global events such as Olympic games, Christmas holidays, St. Valentine’s day, etc., there likely to emerge different methodologies that attempt users to infect computer virus. To protect yourself from different infection damages caused by virus, it is fundamental that never, ever open that attachment files to e-mail for which you do not know. Even it seems to be arrived from one of your friends, it is necessary to carefully check it whether he/she mailed you recently if you feel something suspicious.

(1) The Methodology relevant to “Me-too” Infection

Following are the 2 types of methodologies being identified:

(a) SEO Poisoning (Search Engine Optimization Poisoning)

SEO is the artifice to increment/increase the websites’ order to be displayed based on the result picked by the search engine.

In this method, when you search “Swine” as a keyword, some malicious intent may hide malicious website (s) to be ranked at the high order such as top 3, etc. on that listing resulted by that search engine (Typically, this method is covered under such links in where the word a user interested in or a vogue word as a keyword; this time, we recognized such links in where “swine” is used as a keyword since the swine (H1N1) flu virus is getting renowned.) Accordingly, upon clicking the link, the user will be induced to one of malicious sites in where “swine” is included and exposed by the threat of virus infection.

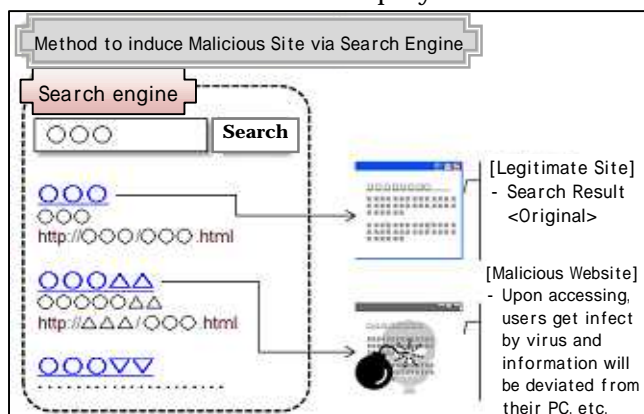


Chart 1-1: Method which induce a user malicious site via search engine

This is the method which exploits user’s behavioral science such as “users are likely to click those sites placed at the top portion of the list resulted by the search engine”, “users easily believe that those sites placed at the top portion of the list are safe”, etc.

<Reference>

The top 10 threats – Information Security White Book 2008, Part II (IPA) (in Japanese)
The 7th: The method which induce a user malware distribution site from the search engine
http://www.ipa.go.jp/security/vuln/20080527_10threats.html

(b) Infected by Virus Exploiting Fictitious Alert

As we already explained earlier in this summary, this method will send such mail appending to the file (this time, it is identified that a PDF (Portable Document Format) files is used as the attachment file) which pose to be the alert for "H1N1" flu virus by a malicious intent masquerading to be an actual research institution or a fabulous organization to have user open it to infect virus by exploiting vulnerability in his/her application software.

In addition, of such mails, there attempt user to infect virus by inducing to malicious site to have user clicks the links directly written in the mail body rather to have user opens the attachment file to e-mail.

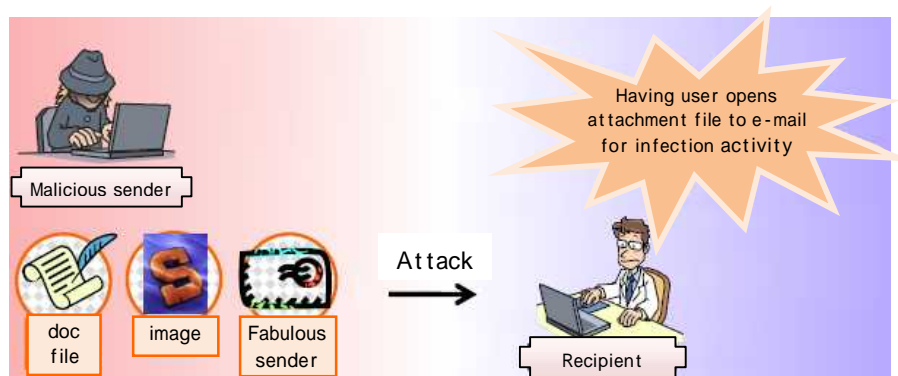


Chart 1-2: Virus Infection Mechanism via a Fictitious e-mail

<Reference>

The top 10 threats – Information Security White Book 2009, Part II (IPA) (in Japanese)
 The 3rd: Spear Type of Attack Getting Sophisticated
<http://www.ipa.go.jp/security/vuln/10threats2009.html>

(2) Virus Overview which Appended to Fictitious Alert

Recently, IPA had acquired one of fictitious alert actually floated around to parse the virus being attached: we identified following behaviors, therein.

Trojan.Pidief.C

This is the virus which infects Windows computers by exploiting the vulnerability either in Adobe Reader or Adobe Acrobat, the application software that enables to browse PDF files. However, the vulnerability is already resolved both in their latest versions (their latest versions are both in 9.1.1 as of May 2009) so that they are virus-free now.

<Reference>

“JVND-2009-01131 Vulnerability in Adobe Reader and Adobe Acrobat Allows to Execute Arbitrary Codes” (JVN iPedia, the database for anti-vulnerability measures information) (in Japanese)
<http://jvndb.jvn.jp/ja/contents/2009/JVND-2009-001131.html>

When infected by Trojan.Pidief.C by opening the PDF being appended, the other virus so called Trojan-Proxy.Win32.Agent.blp will be automatically installed and dummy PDF document will be displayed thereby (See the Chart 1-3). Because of this, it makes users hardly recognizable that he/she is infected by virus. In addition, the Trojan-Proxy.Win32.Agent.blp accesses to malicious site (s) and downloads different virus (s) automatically.

For your information, the Trojan.Pidief.C parsed by IPA does not infect if the vulnerability is resolved so that any of dummy PDF is not displayed, accordingly (See the Chart 1-4).



Chart 1-3: Dummy PDF Displayed by Virus

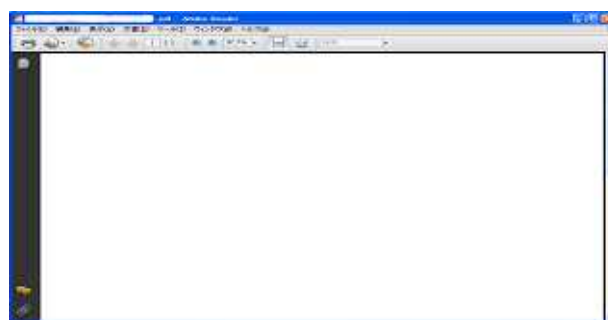


Chart 1-4: Virus-Free

<Reference>

“Be Cautious with the mail masquerading to be a public organization!!” (April 2008)
http://www.ipa.go.jp/security/english/virus/press/200804/E_PR200804.html

In addition, the virus so called Trojan.Win32.Chifrax.a is also detected. This virus was initially detected on October 2007; however, the specimen parsed by IPA this time is the virus somewhat differently reconstructed. The virus can behave as a key logger. The key logger is the program which logs information input by a keyboard to exploit individual information.

(3) Countermeasures

(a) Tips how to distinguish suspicious sites and mails

In the case of (a) SEO Poisoning in the (1) above, it is not easily assumable if the links listed by the search engine is either safe or malicious. However, if either the site or link listed by the search engine does not relevant to the keyword you'd input or you feel somewhat suspicious, be sure not to click to either the site or link to go further.

IPA has started to diagnose such risks relevant to websites on behalf of general computer users. For further information, please refer to the following URL.

<Reference>

IPA has started Website Information Service Based on the “System for Malicious Site Identification and their Countermeasures Information (TIPS)” (IPA) (in Japanese)
<http://www.ipa.go.jp/security/isg/tips.html>

In the case of (b) fictitious alert inclusive of spams in the (2) above, be sure not to open the mail or do not click the link (s) in the mail body directly if you receive a mail from those you do not get in touch with frequently. If available, be sure to communicate with the (expected) sender to check if he/she recently sent you a mail. However, upon communication, do not use the contact address written in the mail body: we encourage you to communicate with the sender by phone as possible as you can.

Further, if one or more files are appended, be sure to check even if the sender you used to exchange mails with. As with the case, it is very much unlikely to receive alert unexpectedly from those you do not get in touch with. Accordingly, the best countermeasure is never, ever open the mail and immediately delete it if you feel somewhat suspicious.

In the case of fictitious alert explained in the (2) above, the malicious intent attempted to infect virus exploiting vulnerability either in the Adobe Reader or Adobe Acrobat; you are to resolve vulnerability in your application software as possible as you can, accordingly.

<Reference>

“Emergency Information – Vulnerability in Adobe Reader and Acrobat” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/ciadr/vul/20090311-adobe.html>

Herein IPA, we provide the consultation window relevant to the mails which target information exploitation shown in the instances in the earlier part of this report for general computer users.

<Reference>

Consultation Window for Suspicious Mails Sent to Specific Organization for Information Exploitation - “Fushin Mail 110” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/virus/fushin110.html>

(b) Fundamental Anti-virus Measures

It is obvious that it is hardly distinguishable that which site is safe, what mail is trustful, etc. nowadays: accordingly, we are not uncertain when, how we will be infected by virus and by what mean, etc. To that end, be sure to conduct following measures as the principle to prevent from infection by virus.

- OSs and application software you are using should always be up-to-dated to resolve vulnerability (ies) as possible as you can.
- The virus signature for your anti-virus measures software should always be up-to-dated to maximize its virus detection capability.
- In case you are infected by virus, important data should be periodically stored in the outside memory media such as USB memory, add-on HDD, etc. separately.

<Reference>

“The Procedure How to Use Microsoft Update and Windows update” (Microsoft)

<http://www.microsoft.com/japan/athome/security/mrt/wu.mspx>

“JVN iPedia – Database for Vulnerability Information Measures” (JVN)(in Japanese)

<http://jvndb.jvn.jp/>

(c) Post-infection Responses

If you got damage caused by virus infection, be sure to check with or without virus in your computer with the anti-virus software you are using: however, do not forget to update the virus signature in the anti-virus software in advance. If you feel that your computer still behaves improperly even you could successfully remove virus, be sure to conduct “System Restoration”. This is the default function for Windows XP, Windows Vista, etc. that can restore the computer information to the sound state the one stored at the specific time/date in the past. For your information, documents created, information for in- and out-bound mails, access history to homepages, and my favorites from the specific time/date in the past to present will be remained as they are. Please refer to the following URLs provided by Microsoft when you conduct “System Restoration” for your computer.

<Reference>

“Using System Restore” (Microsoft)

<http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx>

“Explanation for System Restoration – Windows Vista” (information quoted from “PC Talk” by Microsoft) (in Japanese)

<http://support.microsoft.com/kb/934854/ja>

If the system restoration is not properly done, you are to restore your computer to the state when you initially purchased (initialization). As for actual procedure, please refer to how to

“restore your computer to the initial state when you purchased the computer” column in your instruction manual in case you have to conduct initialization. For your information, be sure to store important data in the outside memory media such as USB memory, add-on HDD, etc. separately for your further security. In addition, be sure to check with or without virus rightly before you back them again to your computer.

<Reference>

Seven anti-virus requirements for computer users (IPA) (in Japanese)

<http://www.ipa.go.jp/security/antivirus/7kajonew.html>

IPA – The Five Anti-Spyware Measures for Computer Users (IPA) (in Japanese)

<http://www.ipa.go.jp./security/antivirus/spyware5kajyou.html>

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

The detection number of virus in May was about 115T: 26.1% decreased from about 156T in April. In addition, reported number of virus in May was 1,387: 3.5% decreased from 1,438 in April.

(¹) Detection number: Reported virus counts (cumulative) found by a filer.

(²) 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 May, the reported number was 1,387 and the aggregated virus count was about 115T.

The worst detection number was for W32/Netsky with about 97T, W32/Downad with about 6T and W32/Mydoom with about 4T subsequently followed.

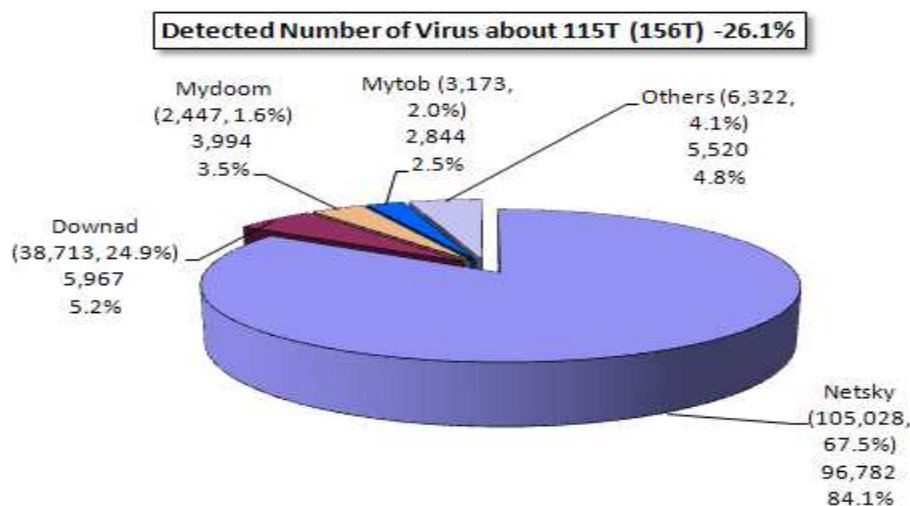


Chart 2-1: Detection Number of Virus
(Note: Numbers in parenthesis are for the previous month)

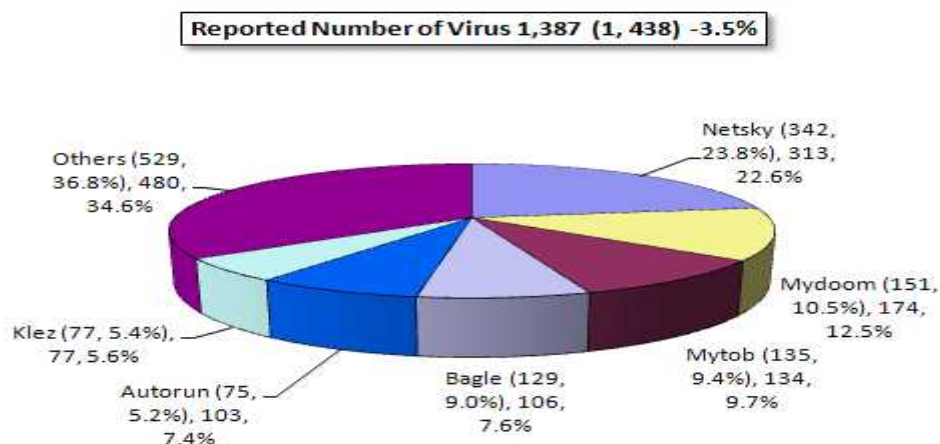


Chart 2-2: Reported Number of Virus

(Note: Numbers in parenthesis are for the previous month)

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

	Dec.	Jan. '09	Feb.	Mar.	Apr.	May
Total for Reported (a)	10	10	9	20	9	8
Damaged (b)	7	7	6	13	6	6
Not Damaged (c)	3	3	3	7	3	2
Total for Consultation (d)	38	29	35	40	39	45
Damaged (e)	19	13	14	11	11	16
Not Damaged (f)	19	16	21	269	28	29
Grand Total (a + d)	48	39	44	60	48	53
Damaged (b + e)	26	20	20	24	17	22
Not Damaged (c + f)	22	19	24	36	31	31

(1) Reporting Status for Unauthorized Computer Access

Reported **number in May was 8**: Of 6 was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was 45(of 1 was also counted as reported number): Of 16 was the number actually damaged.

(3) Status of Damage

The breakdown for damage reports included intrusion with 4, unauthorized mail relay with 1 and DoS attack with 1.

As for the damages caused by intrusion were embedding of fraudulent script within web pages with 3, fraudulently browsed/alterd individual information within web pages with 1, etc. The causes for intrusion were: the computer used for web updates were somewhat infected by virus and FTP account information may be theft thereby with 2, conducted by password cracking attack to website with 1, etc. (as for the other case, the cause has not yet been indentified)

* Password Cracking: The activity to analyze/parse the other person's password illegally. Brute Force Attack (Exhaustive Search Attack) and Dictionary Attack are the well-known methods. The program for cracking activity is also existed.

(4) Damage Instance

[Intrusion]

(i) Fraudulent script was embedded within web pages...

Instance	<ul style="list-style-type: none"> -When I accessed to our business site, my anti-virus software alerted virus. -Study was conducted: it was realized that fraudulent script was embedded in about 100 html files and js files in our business site. Those computers who accessed/browsed our site that had been altered were automatically sent to the malicious site that was not relevant to us in where such trap which automatically downloads virus exploiting vulnerability in the user's applications. -According to the FTP logs, such fraudulent alteration activity was conducted FTP access to web pages thereby. The cause why the FTP account and the password theft have not yet identified, it can be assumed that the computer used for web page updates was somewhat infected by virus. -We changed FTP log-in password, however, again it was altered in vain: we restrained to the FTP access from outside other than authorized IP address, accordingly.
----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[Unauthorized Mail Relay]

(ii) The server was exploited as the steppingstone server for spam relay...

Instance	<ul style="list-style-type: none"> -My business received more than 3,000 spams less than a day. More than a half of them were blocked by the server as spams. However, we realized intermittently accesses thereafter. -Study was conducted: it was realized that the address was not for our business, but was such address exploited as spam relay. There identified failure in our configuration that can block spam relay so that our server allowed them. -Firewall was previously used to block to such spam relay; however, it seems that the UTM*, currently replaced was not properly configured.
----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

* UTM (Unified Threat Management): The function which manages unified threat or such a device itself. Multiple functions such as firewall, intrusion detection protection, address filtering, virus detection, etc. are unified within single device.

IV. Accepting Status of Consultation

The gross number of consultation in May was 1,765. Of the consultation relevant to “One-click Billing Fraud” was 628 (April: 572), consultation relevant to “Hard selling of falsified anti-virus software” was 2 (April: 3), consultation relevant to “Winny” with 5 (April: 4), were realized. (The consultation relevant to “the suspicious mail sent to specific organization to collect specific information/data” was 5 (April: 0).

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

	Dec.	Jan. '09	Feb.	Mar.	Apr.	May
Total	839	960	1,051	1,406	1,668	1,765
Automatic Response System	458	529	521	758	962	992
Telephone	331	390	472	597	651	710
e-mail	49	39	57	49	55	58
Fax, Others	1	2	1	2	0	5

*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 (d) column of the Chart in the “III. Reported Status for Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

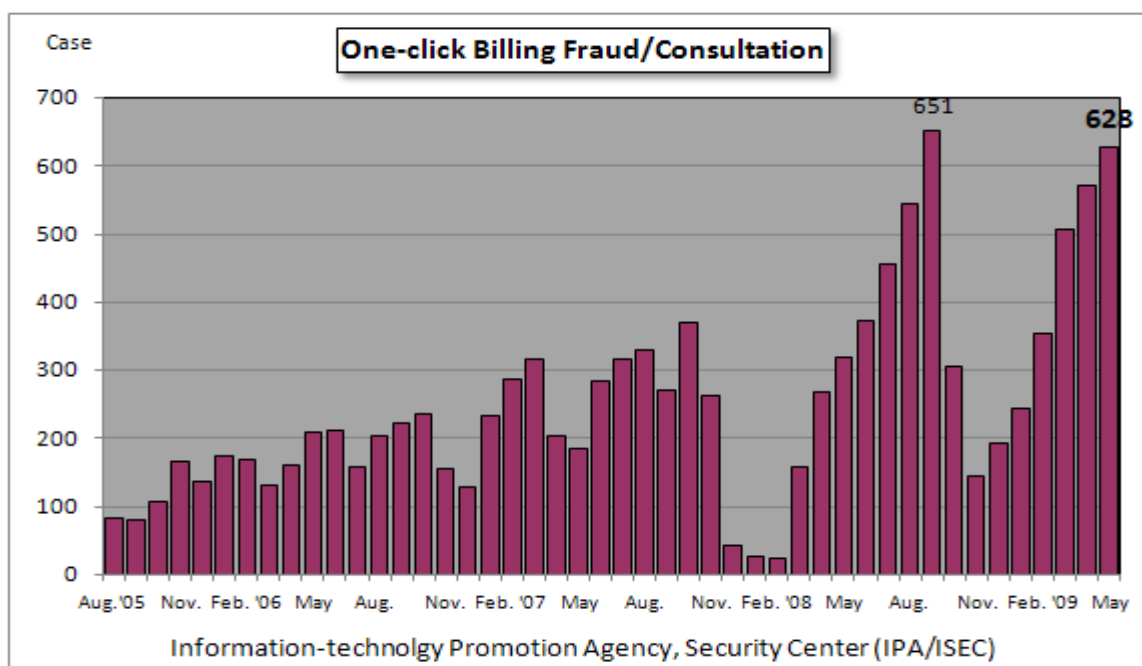


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) I may be fraudulently accessed in an online game site...?

<p>Consultation</p>	<p>I am subscribing charged services in an online game site. One day, I was realized that the accumulated points that can be used as a part of cash were automatically used by someone. According to the site manager, he would study logs, etc. if requested by official organization such as police, etc. I consulted with a police, accordingly; they could not investigate as a case if the damage was not reported by the site manager, as the entity actually got damaged. Then, I asked consultation with a consumer center near my area, they suggested me to file it to police. Things do not work out. What shall I do?</p>
<p>Response</p>	<p>In this case, the actual casualty seemed to be the site manager and your damage was considered to be secondary matter. Accordingly, it is important to have the site manager to study about your damage, anyway. If he does not listened to, be sure to have the consumer center to go between to take necessary actions.</p> <p><Reference></p> <p>National Consumer Affairs Center of Japan (in Japanese) http://www.kokusen.go.jp/map/</p>

(ii) Free mail supposed to be free...?

<p>Consultation</p>	<p>I am using one of well-known free mail. I did not use it awhile, but I again start to use it. One day, I received a mail from the free mail manager. According to that mail, "because of such mails that are hardly sortable either legitimate mail or spam so that our server is getting failed. To that end, he has to spend a lot of money to fix it so that he may have to charge it every user equally." Is it real?</p>
<p>Response</p>	<p>It probably is a mail for a fictitious billing from someone masqueraded to be the free mail manager. If you questioned with the mail what it said, we recommend you to inquire the free mail manager directly. If you do that, do not use the address written in that mail body: rather, you'd better to communicate with the enough trustful address which you may be fund in their official home pages, etc.</p> <p>In case you'd already "transferred money" or you are "billed frequently", we encourage you to ask consultation with the police.</p> <p><Reference></p> <p>National Police Agency - Internet Security/Consultation for Safety (in Japanese) http://www.npa.go.jp/cybersafety/</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in May was **115,336** for the 10 monitoring points and the gross number of source* was **36,779**. That is, the number of access was **372** from **119** source addresses/monitoring point/day.

*Gross number of source: the gross number of the source accessed 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.

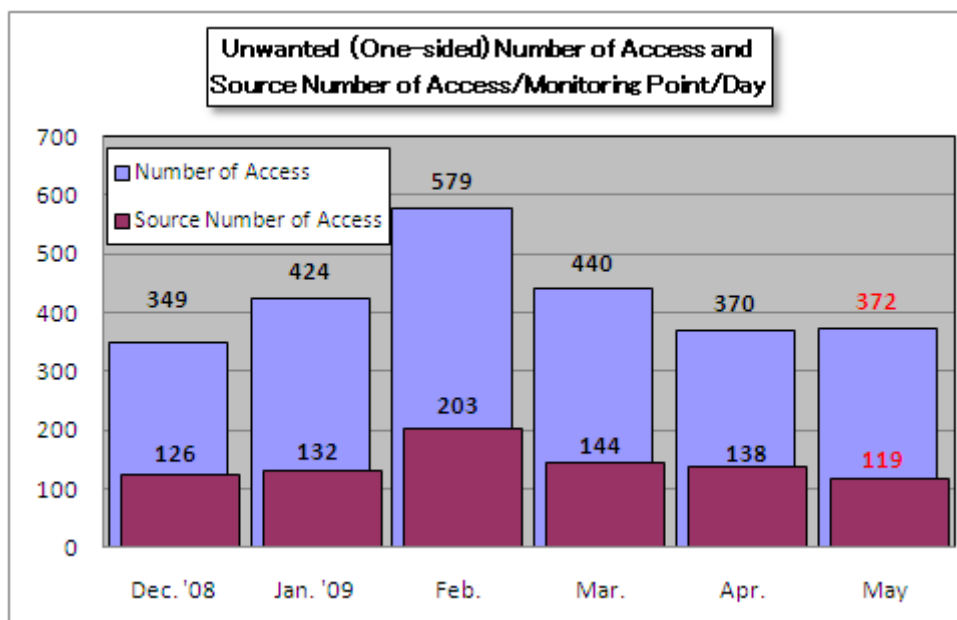


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day

(1) Access to the Port 2967/tcp

The Chart 2-1 shows that the access to the port 2967/tcp tended to increase in the early part of May.

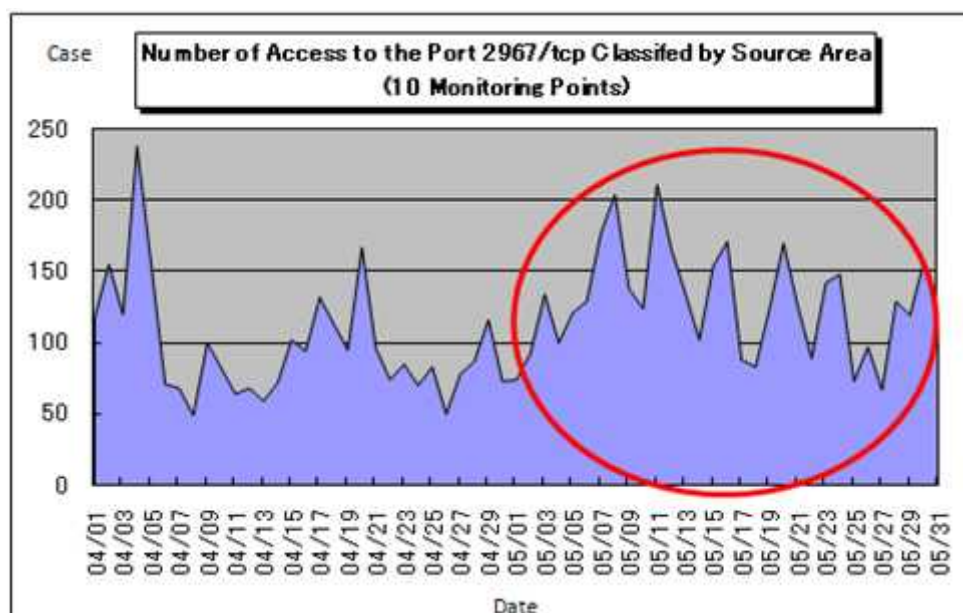


Chart 5-2: Number of Access to the Port 2967/tcp (10 Monitoring Points)

The 2967/tcp is the default port exclusively used by Symantec products. As for the vulnerability in the port likely exploited by attacks, the “Vulnerability in Symantec Client Security and Symantec AntiVirus allows privilege elevation (SYM06-010)” was publicized in the past.

This vulnerability allows attacker to fraudulently acquire/delete files such as Symantec Client Security and Symantec AntiVirus, etc. so that the system is likely to be crushed.

<Reference>

“Symantec Client Security and Symantec AntiVirus Elevation of Privilege (SYM06-010)”
<http://www.symantec.com/avcenter/security/Content/2006.05.25.html>

Accordingly, if the vulnerability in the said products is not resolved, you will likely be attacked exploiting by that vulnerability. To prevent yourself from damage, it is important to be cautious with the information relevant to vulnerability: when information relevant to your products is publicized, be sure to resolve them in your earliest convenience.

For your information, the homepages provided by the vendor for the products you are now using and the portal site for vulnerability information such as JVN are very much helpful: accordingly, be sure to check them periodically to be ready to conduct necessary anti-vulnerability measures on time.

<Reference>

“JVN (Japan Vulnerability Notes)” (portal site for vulnerability information) (in Japanese)
<http://jvn.jp/>

“JVN iPedia - Information database for anti-vulnerability measures information” (in Japanese)
<http://jvndb.jvn.jp/>

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/200905/documents/TALOT2-0905.pdf>

Summary Reporting Status for Computer Virus/Unauthorized Computer Access for December
<http://www.ipa.go.jp/security/english/virus/press/200905/documents/summary0905.pdf>

Attachment_1 Computer Virus Incident Report
<http://www.ipa.go.jp/security/english/virus/press/200905/documents/virus0905.pdf>

Attachment_2 Unauthorized Computer Access Incident Report
<http://www.ipa.go.jp/security/english/virus/press/200905/documents/crack0905.pdf>

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

@police: <http://www.cyberpolice.go.jp/english>

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