

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

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

I. Reminder for the Month

**“Do not fail to conduct daily security measures! Viruses are being evolved day by day!”
- Viruses multi-functionality is further escalated -**

The reports to IPA relevant to the virus so called W32/Virut is gradually increased from the end of 2008. Since the virus was initially reported to IPA in August 2006; accordingly, it was not a recently emerged virus: however, its variant (s) for which infection/dissemination function being enhanced is further activated ever before: it can be considered that the infection activities by this virus is getting enlarged.

What if your computer is infected by W32/Virut, the system files for Windows that need to behave properly will be destructed so that it is hard to get it back to the normal state.

To prevent such damage caused by virus, it is fundamental to resolve any of vulnerabilities in your computer with Windows Update, etc. and to conduct adequate security measures utilizing anti-virus software, etc. In case you would face damage caused by virus, it is necessary to back up your important data to outside media such as USB memory, etc regularly.

(1) The feature of W32/Virut

The reported number of W32/Virut to IPA is usually ranked as one of the worst 10 viruses every month over the last year. In addition, it is realized that the number of W32/Virut variants were detected from the reports summarized by the other organizations.

<Reference>

“The alerting activities by Cyber Clean Center for December 2008 – Achievements” (in Japanese)

<https://www.ccc.go.jp/report/200812/0812monthly.html>

Based on the outcome of the W32/Virut variant parsed by IPA, following features are identified. The virus features to infect and spread it over to enlarge its scoping activities over and over.

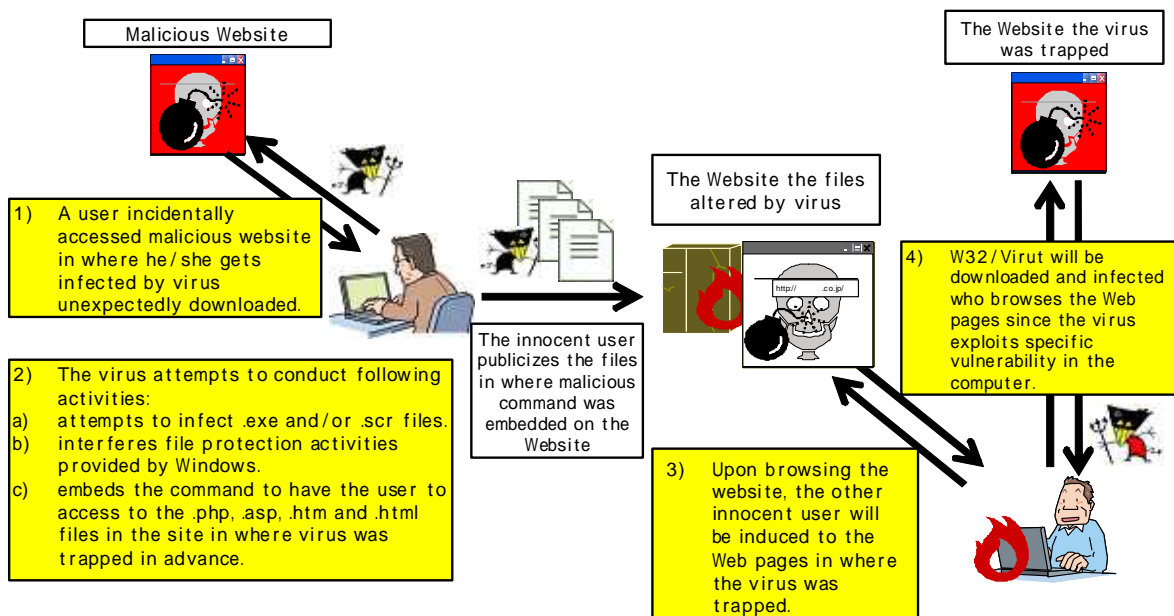


Chart 1: W32/Virut Infection Activities

- (a) The W32/Virut is initially infected by following procedures: a user unexpectedly downloads and gets infected by the virus from a malicious Website in where the user incidentally induced [1] in the Chart 1.]. The virus infected to the user attempts to conduct infection activities to the files that has “exe”^{*1}, “scr”^{*2} extensions [2]-a in the Chart 1.]. However, the virus will not infect to program files otherwise the virus itself will get troubles to behave NEATLY.

*1 exe: The extension which presents execution type of programs and applications.

*2 scr: The extension which presents screen saver used by Windows.

- (b) The virus infected attempts to embed the commands to the files that have “php”, “asp”, “htm” and “html” extensions to have users access to the Website in where W32/Virut virus is trapped in advance for its dissemination activities [2]-c in the Chart 1.]. Since these files will mainly be used to create homepages, an innocent user will upload/publicize his/her homepages along with the malicious commands. What if the other innocent user accesses to that homepage; the user will also get infected by W32/Virut [3] in the Chart 1.]. In the meantime, W32/Virut attempts to parse if there is specific vulnerability in the computer who browsed/accessed the homepage: if any, the virus infects to that computer by exploiting the vulnerability [4] in the Chart 1.].

Please remember that in this way, W32/Virut will cause damage not only to the computer initially infected, but also to the computers induced to the homepage in where the virus is trapped in advance.

(2) The major damages

According to the result parsed by IPA, it is identified that the W32/Virut variant will cause following damages.

- (i) Infection will be enlarged to the program files as well as screen saver files in the (infected) computer.
- (ii) The virus interferes the file protection function^{*3}, the default function provided by Windows.
- (iii) The virus disables the firewall configuration provided by Windows.
- (iv) The virus attempts to embed the commands to the files that have “php”, “asp”, “htm”, and “html” extensions which automatically send users to malicious Website in outside: accordingly, the files will be altered.

*3 Windows file protection: One of default functions provided by Windows. This function protects those files necessary for Windows to behave properly from automatic alteration activities.

As the consequence (i) above, as the number of files infected will be increased, their removal activities will also be getting hard. In the event of (ii) above, the infection activities to the system files needed for Windows to behave properly cannot be blocked adequately; accordingly, the computer may behave unstably. Because of (iii) above, expected security features will not be provided so that the computer will confront certain risks. What if someone created/publicized his/her homepage in where malicious command was embedded, (iv) it is possible that the user (s) who browsed/accessed that homepage will also get damaged.

If damaged, your computer may not get back to the previous/sound state: accordingly, the last resort to get back to the normal state is to initialize your computer when you purchased as the restoration activity from the damage caused by virus such as W32/Virut, etc. is not simple.

(3) Countermeasures

- (a) Infection prevention measures

First of all, be sure to check that your virus signature in your anti-virus software always

up-to-dated. It also is necessary that the virus detection function should always be effective. Since W32/Virut initially parses if the targeted computer has specific vulnerability: if any, the virus starts infection activities. Accordingly, the first thing you are to do is to resolve vulnerabilities as far as possible and to maintain your OSs and/or application software always up-to-dated. In addition, be sure to back up your important data to the virus-free outside memory media such as USB memory, CD-R, add-on HDD, etc. to start restoration activities swiftly in case infected/damaged.

(b) Post-infection responses

As we described it in the (2) above, getting back your computer to the previous/sound state may not be possible if damaged. Although you can perfectly remove the virus and your computer can be restored to the previous state, the virus activities may not be perfectly terminated: it can be identified that W32/Virut shifts to different virus when removed*. It is identified that the virus being shifted may carry such function which downloads different viruses while users do not know. This means when infected by W32/Virut, nobody can accurately analyze how far the virus can cause damage. With the reasons above, when infected by W32/Virut, we encourage you to initialize your computer to the original state before you purchase it. As for actual initialization activities, be sure to follow to the procedure described in the "How to restore your computer" attached to your computer when you purchased. In addition, never fail to check with or without any viruses in the data you'd backed up with your anti-virus software before restore them to the computer successfully recovered.

*W32/Virut may infect/append the other viruses: when removed, the residual virus (es) is appeared/executed, accordingly.

<Reference>

IPA - The Seven Anti-virus Requirements for Computer Users

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

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

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

IPA - The description of anti-Bot measures (in Japanese)

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

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

The detection number in February was **about 128T** (January: about 159T): decreased 19.1%. In addition, the reported number in February was **1,463** (January: 1,860): decreased 21.3%.

- (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 February, the reported number was 1,463 and the aggregated virus count was about 128T. *(From the May '08 report, we use "T (thousand)" instead of using "M (Million)" to specifically present the detection number of virus.)*

The worst detection number was **W32/Netsky** with about **113T** and **W32/Mytob** with about **5T** and **W32/Mydoom** with about **2T** subsequently followed.

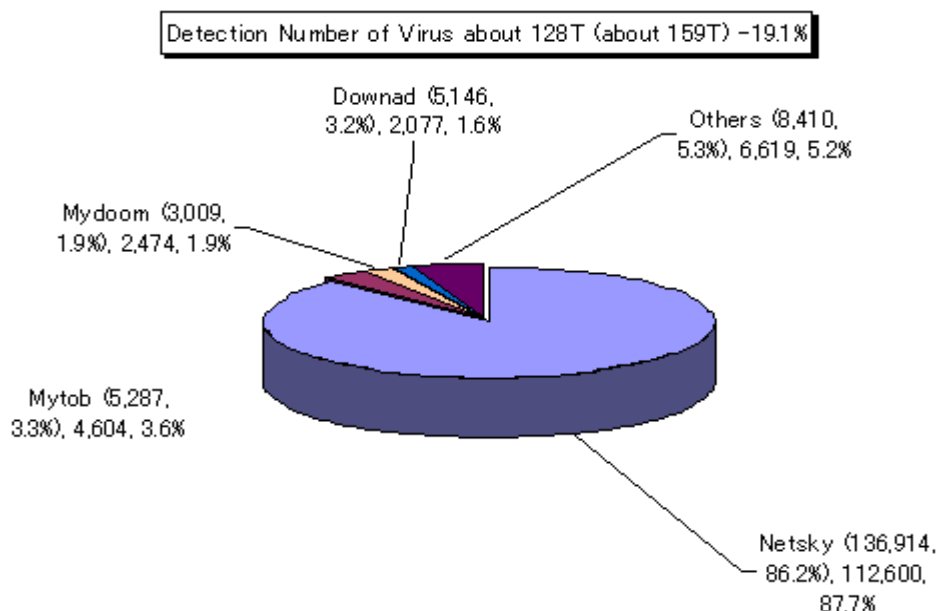


Chart 2-1: Detection Number of Virus (Numbers in parenthesis present the figures in previous month.)

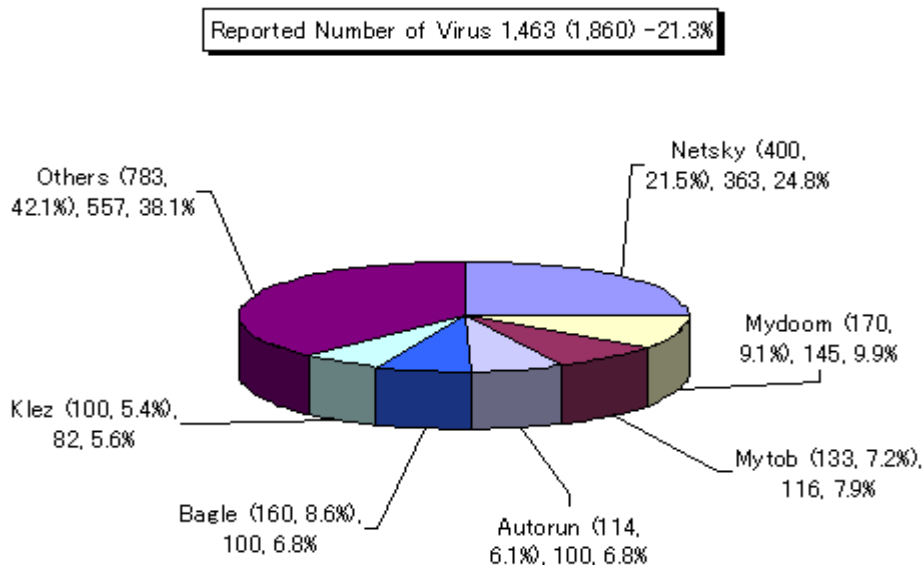


Chart 2-2: Reported Number of Virus (Numbers in parenthesis present the figures in previous month.)

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

	Sep.	Oct.	Nov.	Dec.	Jan. '09	Feb.
Total for Reported ^(a)	14	17	18	10	10	9
Damaged ^(b)	12	12	12	7	7	6
Not Damaged ^(c)	2	5	6	3	3	3
Total for Consultation ^(d)	38	58	39	38	29	35
Damaged ^(e)	20	22	19	19	13	14
Not Damaged ^(f)	18	36	20	19	16	21
Grand Total ^(a + d)	52	75	57	48	39	44
Damaged ^(b + e)	32	34	31	26	20	20
Not Damaged ^(c + f)	20	41	26	22	19	24

(1) Reporting Status for Unauthorized Computer Access

Reported number in February was 9: 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 35 (of 2 was also counted as reported number): Of 14 was the number actually damaged.

(3) Status of Damage

The damage report included: by **intrusion** with **1**, by **DoS attack** with **1**, by **source address spoofing** with **3** and by **embedding of malicious codes** with **1**.

The major damage caused by “intrusion” was that the data in a database was altered by SQL injection attack. Because of this attack, some vulnerabilities were exploited which allowed intrusion was the major cause. As for “source address spoofing”, someone spoofed to be a legitimate user logged in and used on-line services (on-line games with 2, communication site with 1) without asking.

***SQL (Structured Query Language):**

The query language used to operate/define data in the relational database management system (RDBMS).

***SQL Injection:**

One of attacking methods exploiting vulnerability (ies) in the program which accesses to a database: this attack fraudulently browses and/or alters data within that database with the methods other than legitimate.

(4) Damage Instance

[Intrusion]

(i) Data was altered by SQL injection attack...

Instance	<ul style="list-style-type: none">- When I was doing maintenance activities, I realized that some suspicious scripts were added so that the data within a database was altered. The database was used to showcase/catalog our products on Website.- Study was conducted: it was realized that the database was altered by SQL injection attack. Further, the (suspicious) scripts being added may automatically download virus to the client (user) who browsed/accessed to our site.- Because of the number of accesses caused by SQL injection attack, the Web server performance was getting lowered so that some clients experienced hard time to access/browse to our site.- Accordingly, we exclusively provided users and/or clients who accessed/browsed to our site following information on our Web pages: the potential that the users and clients would be infected, how to check with or without the virus, etc.
----------	--

IV. Accepting Status of Consultation

The gross number of consultation in February was 1,051. Of the consultation relevant to “One-click Billing Fraud” was 355 (January: 243), consultation relevant to “Hard selling of falsified anti-virus software” was 17 (January: 11), consultation relevant to “Winny” with 7 (January: 8), were realized. (The consultation relevant to “the suspicious mail sent to specific organization to collect specific information/data” was 5 (January: 0).

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

	Sep.	Oct.	Nov.	Dec.	Jan. '09	Feb.
Total	2154	1171	713	839	960	1,051
Automatic Response System	1302	677	363	458	529	521
Telephone	755	441	288	331	390	472
e-mail	93	47	62	49	39	57
Fax, Others	4	6	0	1	2	1

*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”.

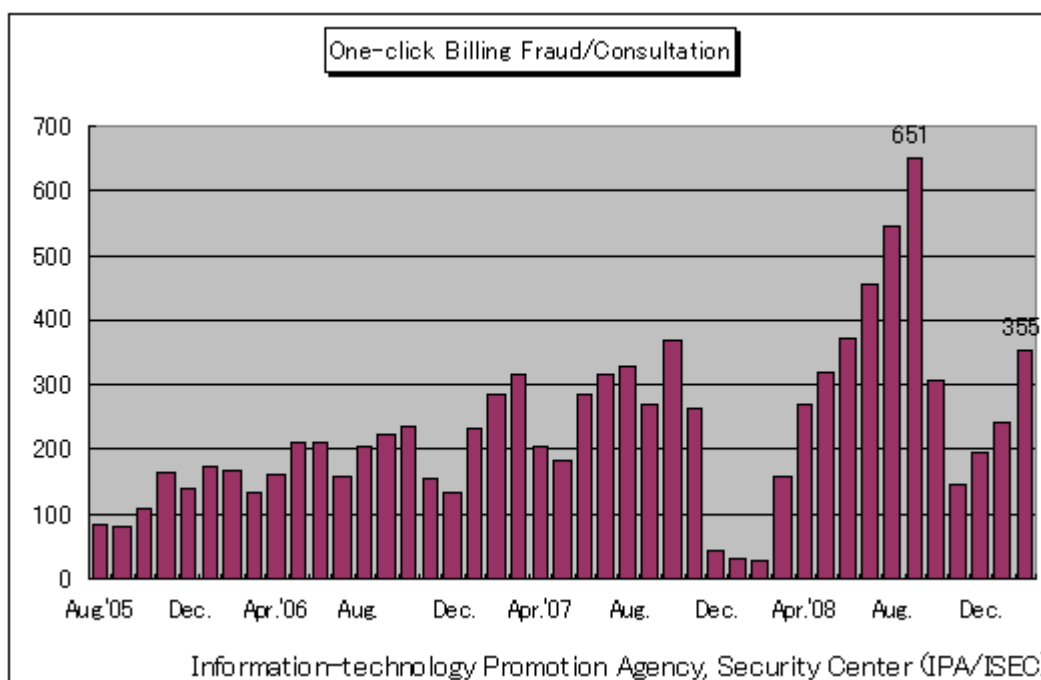


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) Infected by virus via the USB memory my friend gave me...?

<p>Consultation</p>	<p>I'd gotten an USB memory from my friend. My computer does not function well since I inserted it. Looking back, there appeared a foreign icon when I inserted it. I did not apply any anti-virus software on my computer. Accordingly, I checked with or without of virus on one of the on-line checking sites. Since number of virus was detected so that my computer was initialized. What should I do next?</p>
<p>Response</p>	<p>It is probable that there hid one of USB memory infection type of viruses in the USB memory your friend gave you. If the one of USB memory infection type of viruses were hidden while your friend did not know, it is probable that his/her computer too, is infected by that virus. The first thing you have to do here is to ask your friend check with or without of virus in his/her computer.</p> <p>To prevent further infection by virus, be sure to maintain OSs and applications always up-to-dated. Never fail to install anti-virus software and be sure that the virus signatures always up-to-dated.</p> <p>For your further security, be sure to refrain to insert such USB memory, memory card, etc. possessed by the others or a find for which you are not managing.</p> <p><Reference> IPA – Reminder for the month: “Be sure to double-check of your security measures for outside media such as USB memory, etc.!” http://www.ipa.go.jp/security/english/virus/press/200811/E_PR200811.html</p>

(ii) Do not want to update my OSs as I need to use specific software hereafter...?

<p>Consultation</p>	<p>I am a Windows XP SP1 user. I know that the latest version of XP is SP3, but I am still debating whether I need to update or not as I have heard that the software I am using will not be available in the SP3 environment. I do use router, I do exchange every mails in textual format and I never open suspicious mails so that I believe my security measures is perfect! In addition, I'd never discovered suspicious mails in the folder for “sent out mails”. Accordingly, I believe that I'd never ever sent any virus mails to the others.</p>
<p>Response</p>	<p>Since supporting session for Windows XP SP1 by Microsoft was already concluded so that none of modification programs will be provided even if vulnerabilities are found. Accordingly, you may be infected by virus depending on the vulnerability you may have even you are simply linking to the Internet or just browsing a malicious site. Resolving of vulnerability (ies) is the mandatory security measures. In another words, vulnerability is remained, any security measures cannot provide expected security.</p> <p>It must be a “wag the dog” issue if you want to neglect security measures to use specific software from now on. We encourage you to check up your best measures based on that your OSs will be up-to-dated.</p> <p>For your further information, if your computer is exploited as a stepping stone to send vicious mails, none of virus probe will be left in your “sent out mails” folder as virus itself send virus mails directly.</p> <p><Reference> IPA – The Seven Anti-virus Requirements for Computer Users http://www.ipa.go.jp/security/antivirus/7kajonew.html</p>

V. Accessing Status Captured by the Internet Monitoring (TALOT2) in February'09

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in January was **138,944** for the 10 monitoring points and the gross number of source* was **48,671**. That is, the number of access was **579** from **203** 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.

- TALOT2 maintenance periods were fallen on February 6 to 9 so that the monitoring activities were not available during that dates. Accordingly, the monitoring data in February was aggregated excluding these 4 days.

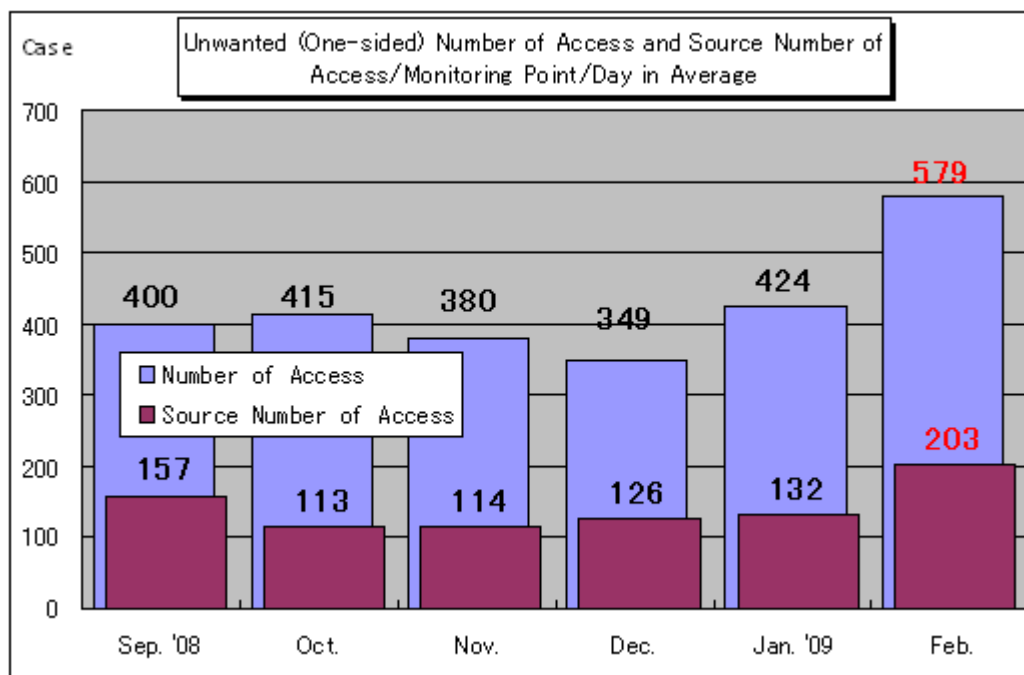


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access (average) and the source number of access (average)/monitoring point/day from September 2008 to February 2009. Both unwanted (one-sided) accesses were significantly increased compared with the one in January.

(1) Access to the Port 2967/tcp

The access to the port 2967/tcp increased from early part of January was further increased in February (See the Chart 5-2.).

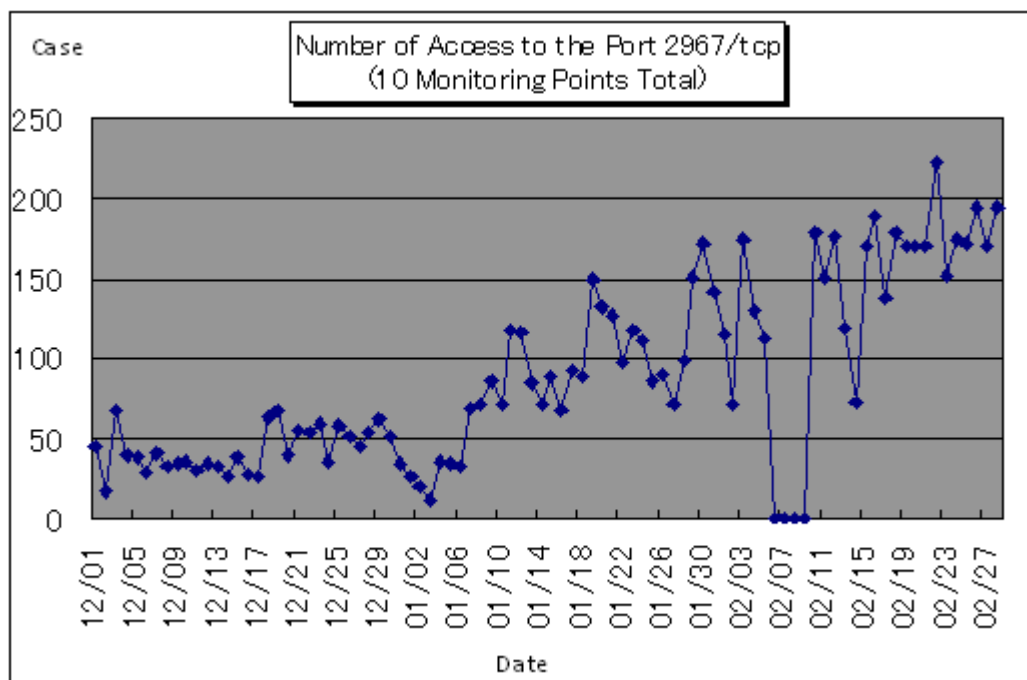


Chart 5-2: Number of Access to the Port 2967/tcp (10 Monitoring Points Total)

2967/tcp is the default port used by Symantec products. The vulnerability relevant to “Symantec Client Security and Symantec AntiVirus which allow privilege escalation (SYM06-010) was publicized in the past.

This vulnerability allows malicious attackers gain/delete specific files in the targeted products such as Symantec Client Security and Symantec AntiVirus, etc. so that they will be no longer available for use (i.e., will be destructed).

<Reference>

Vulnerability in “Symantec Client Security and Symantec AntiVirus Elevation Privilege” (SYM06-010)” (Publicized in May 25, 2006)

<http://www.symantec.com/avcenter/security/Content/2006.05.25.html>

It is probable that the attack targeting this vulnerability is conducted up to current. However, those Symantec Client Security and Symantec AntiVirus users can resolve this vulnerability by updating their signature files utilizing Live Update session provided by Symantec. Accordingly, users should check whether your signature files are up-to-dated. If your supporting period is terminated and you cannot update your signature files, be sure to purchase/apply the latest version of signature files. Be sure to be ready to conduct anti-vulnerability measures for the products now you are using: to that end, it is necessary to check the portal sites relevant to vulnerability information such as JVN, etc. daily.

<Reference>

“JVN (Japan Vulnerability Notes)” (in Japanese)

<http://jvn.jp/>

“JVN iPedia – Database for anti-vulnerability measures” (in Japanese)

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

(2) Access to the Port 445/tcp

Number of access to the port 445/tcp was already monitored in January; however, the access was getting further increased in February (See the Chart 5-3.). As we described in the January report, the access to the port 445/tcp targeting vulnerability in Windows for which information was emergently publicized by Microsoft in October 24, 2008 may still be remarkable.

<Reference>

Internet Monitoring (TALOT2) for January 2009

<http://www.ipa.go.jp/security/txt/2009/documents/TALOT2-0902.pdf>

In the meantime, we analyzed the accessing status for the port before and after the system maintenance period (February 6 - 9), it is identified while the access from domestic was decreased, yet the access from overseas was significantly increased (See the Chart 2-3.).

One reason can be considered is the network segment for IP address was changed before and after the system maintenance period.

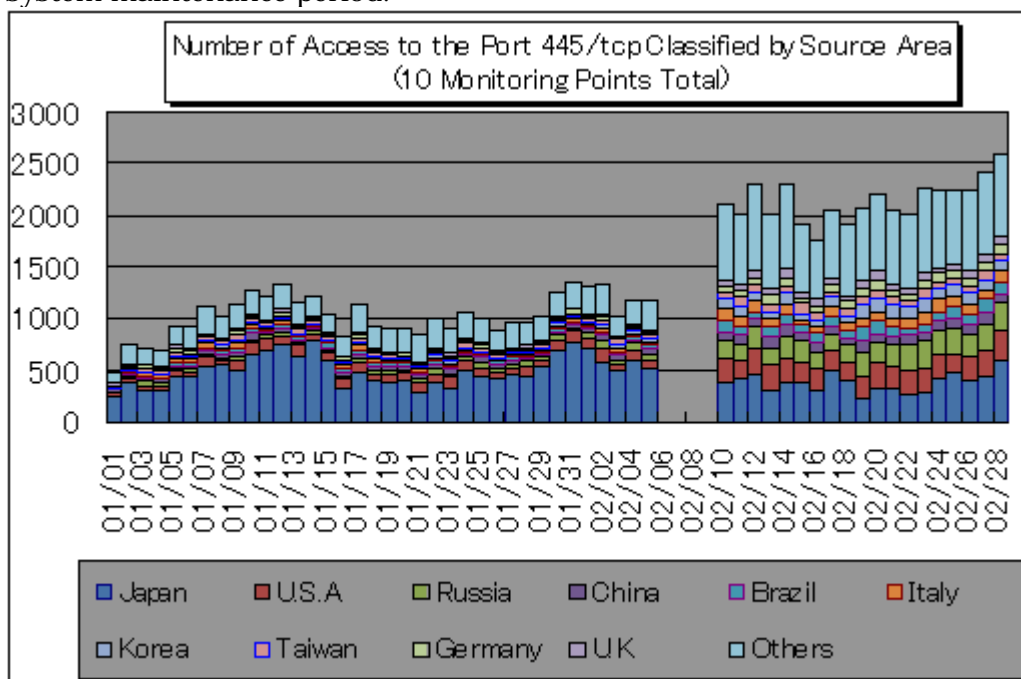


Chart 5-3: Number of Access to the Port 445/tcp Classified by Source Area

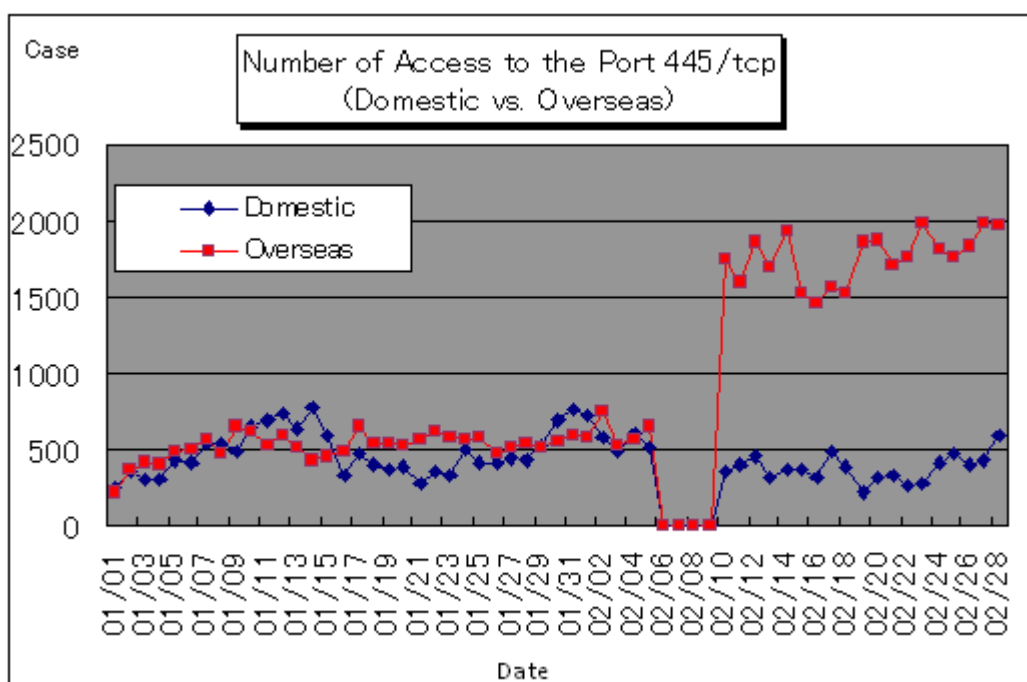


Chart 5-4: Number of Access to the Port 445/tcp (Domestic vs. Overseas)

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

Attachment_3: Accessing Status Captured by the Internet Monitoring (TALOT2)

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/TALOT2-0903.pdf>

Summary Reporting Status for Computer Virus/Unauthorized Computer Access for December

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/summary0903.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/virus0903.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/crack0903.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