

Computer Virus/Unauthorized Computer Access Incident Report – October 2009

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

I. Reminder for the Month

The “Threat relevant to Falsified Security Measures Software” Enlarges Again!
– Be sure to learn malicious intents’ methodologies to prevent potential damages –

According to the virus reports summarized by IPA by every month, such threat that the malicious program (hereinafter, we will refer it as virus) which attempts user to purchase “falsified security measures software” is again enlarged after the interval of about a year (See the Chart 1-1): The “falsified security measures software” refers the virus which warns user fictitious messages such as “Your computer is infected by virus”, etc. This virus also displays the fabulous window relevant to “virus detection”: This window urges the user to purchase paid-for “security?” product to remove virus. Eventually, the user will be led to a malicious site to buy “falsified security measures software”.

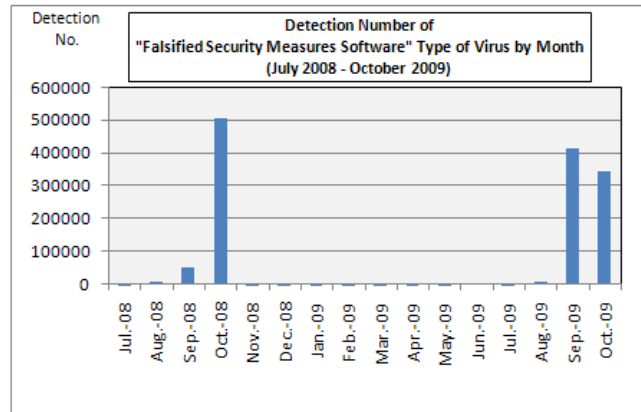


Chart 1-1: Detection Number of “Falsified Security Measures Software” Type of Virus by Month (Jul. 2008 – Oct. 2009)

To prevent potential damages caused by this virus, be sure to check the methodology (ies) used by this anew “falsified security measures software” type of virus for which we’d specifically describe below.

* Detection Number: The gross total of the virus (pcs.) found by users and then filed by IPA.

(1) Infection Mechanism

As for the infection mechanism, following instances are identified as the methodologies used by the “falsified security measures software” type of virus:

(i) via the file (s) appended to spam:

It can be assumed that there distributed/spread spams that masqueraded to be Microsoft and/or one of renowned businesses in overseas extensively wide area (see the Chart 1-2). Accordingly, if user opens the file appended to that spam either intentionally or by mistake, the virus (i.e., downloader) which embedded in the file automatically downloads/installs the “falsified security measures software” type of virus from the site (s) outside while the user does not know; (see the “step 1-1 to 1-3” in the Chart 1-3).

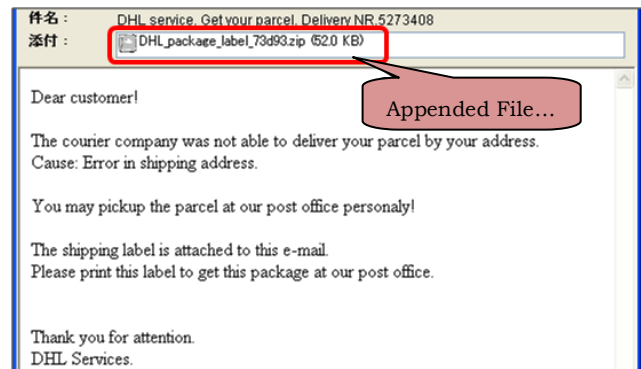


Chart 1-2: Example of the spam identified by IPA masqueraded to be the one of renowned businesses in overseas***

<Reference>

“Alert: Be cautious with the malware which may have been appended to the spam spoofing to be Microsoft” (Publicized on October 20, 2009) (JPCERT/CC) (In Japanese)
<http://www.jpCERT.or.jp/at/2009/at090022.txt>

(ii) Upon browsing one of the legitimate websites in where wrongful scripts are previously embedded:

In this methodology, when user attempts to browse one of legitimate websites, the “falsified security measures software” type of virus will be automatically downloaded/installed to his/her computer since wrongful scripts (program) was already embedded to the legitimate site by malicious intent (see the “step 2-1 to 2-5” in the Chart 1-3). In this case, such vulnerability (ies) in the user’s OSs and/or applications such as Adobe Flash Player, Adobe Reader, etc. will be exploited by the virus (i.e., malicious intent).

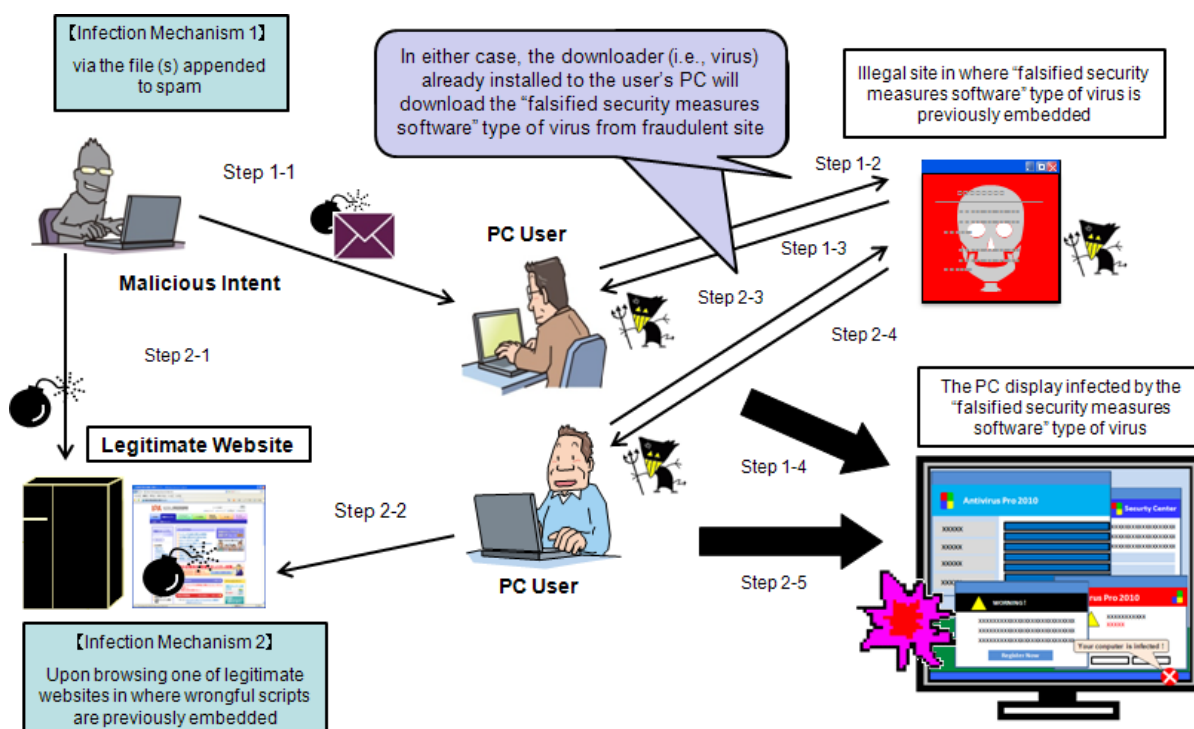


Chart 1-3: Infection Mechanism used by the “Falsified Security Measures Software” type of Virus

(2) Preventive Measures

To prevent potential damages caused by the “falsified security measures software” type of virus, be sure to conduct following measures:

(a) Spam handling:

The best security measures against the virus masquerading to be the one of substantiated/reowned organizations such as Microsoft, etc. being appended to spam to have you make it trust such as in the (i) in the “(1) Infection Mechanism” above is “never, ever opens the mail which you think you are not related to”. It depends, but it is also helpful to immediately contact to the organization (i.e., supposed to be the source of the sender) to verify the authenticity. It is utmost important to pay close attention to prevent infection from virus if you feel somewhat suspicious.

(b) Vulnerability measures:

As with the (ii) in the “(1) Infection Mechanism” above, you may get damage even you simply browse legitimate website (s) in where wrongful scripts are previously embedded: in this case,

the vulnerability (ies) in your OSs and/or applications are already exploited by malicious intent. Further, if the vulnerability (ies) in the computer to be used for editing web pages is not resolved, you will give malicious intent a chance to embed wrongful scripts so that you may cause those users who browse that web pages. As you will see, the fundamental preventive measures is to maintain your OSs and applications always up-to-dated and to resolve vulnerability (ies) as far as you can.

(c) Anti-virus measures:

As for the common preventive measures along with the individual preventive measures mentioned in the (a) and (b), it is also important to update your trustful anti-virus software upon use. If you are going to purchase anti-virus software, be sure to pick up the one provided by an enough trustful provider. To that end, we encourage you to purchase it at a retailer, etc. directly rather downloading it via the Internet.

(3) The Symptoms

Upon verified the “falsified security measures software” type of virus obtained by IPA, we identified following symptoms:

- There emerges an “X” icon on the task bar which insistently pops-up such alert that “Your computer is infected by virus!”.
- The display for “Antivirus Pro 2010” which anyway seems to be a security measures software suddenly appears and automatically starts to check with or without of virus in your computer. Upon it is through, such falsified message saying “there identified number of viruses in your computer” is appeared and the user is urged to purchase certain (?) security measures software to remove them frequently (till the user actually purchase it!).
- Somewhat “Security Center” look like display for Windows in English environment is appeared and warn you about the security relevant issues in your computer and urges to purchase certain (?) security measures software.

These symptoms are appeared on the display in concert (see the Chart 1-4) and the user is eventually misled to enter his/her personal information such as credit card number, etc.

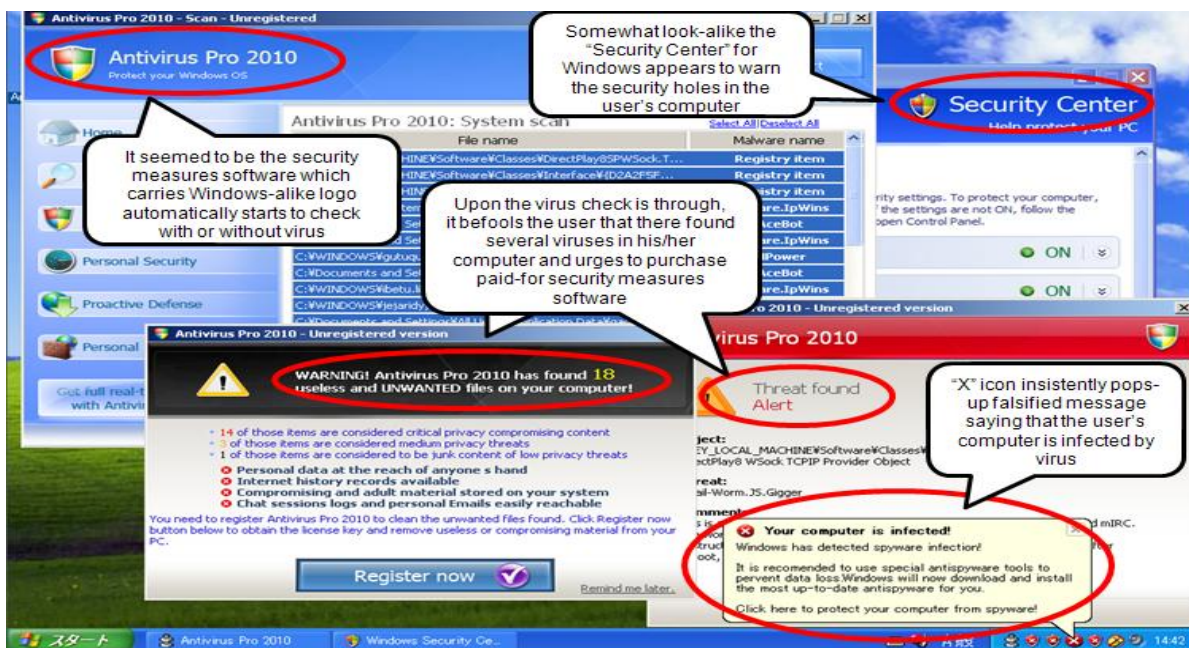


Chart 1-4: The Windows Display Infected by the “Falsified Security Measures Software” type of Virus

As you can easily imagine that trustful anti-virus measures software does not urgently alert in this way. In case your computer anomaly behaves like the example in the Chart 1-4, it is probable that your computer is get infected by the “falsified security measures software” type of virus: The potential cause may be your anti-virus software which is not regularly up-to-dated. The virus may furnish variety of blocking mechanisms against anti-virus software. Accordingly, they may be remained in your computer even you up-to-date your anti-virus software to remove the virus. In case such symptoms do not remedied, be sure to refer to the “(4) Post Countermeasures” which described below.

(4) Post Countermeasures

In case the symptoms do not remedied with the anti-virus software up-to-dated, be sure to conduct “System Restore” which will be specified in (a) below. If the symptoms are still remained in vain or the “System Restore” is failed, be sure to initialize your computer as the last resort.

(a) Recovery by “System Restore”:

Windows XP, Windows Vista, and Windows 7 furnish “System Restore” function that can restore back to the previous state either before the computer unstably behaves or the computer is getting unavailable. This is the default function which recovers the computer’s state based on the system information the Windows automatically and routinely stores.

Upon conducting the “System Restore”, be sure to refer to the following URLs provided by Microsoft. Please be noted, those application software installed, the information updated from the date you’d specified to today will be unavailable so that you need to do that again after the “System Restore” is successfully completed.

<Reference>

“Using System Restore” (Microsoft)

<http://www.microsoft.com/windowsxp/using/setup/support/sysrestore.msp>

“How to Restore the System for Windows Vista” (Information cited from the “PC talk” by Microsoft) (in Japanese)

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

“The Feature of Windows 7: System Restore” (Microsoft) (in Japanese)

<http://windows.microsoft.com/ja-JP/windows7/products/features/system-restore>

(b) Computer Initialization:

This refers to initialize your computer to the original state when you just purchased it. Upon initialize your computer, be sure to follow to the procedures in the “restoring to the computer just purchased” described in your instruction manual. As always, we recommend you to back up important data to the outside memory media such as USB memory, CD-R, or add-on HDD, etc. for your further security.

<Reference>

Seven Rules of Virus Countermeasures for PC Users (IPA)

<http://www.ipa.go.jp/security/english/virus/antivirus/7RulesV.html>

Five anti-spyware requirements for computer users (IPA) (in Japanese)

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

Five must-dos for dealing with files attached to e-mail (IPA) (in Japanese)

<http://www.ipa.go.jp/security/antivirus/attach5.html>

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

(1) Reporting Status of Virus

The detection number of virus in October was about 70T: decreased about 7.8% from the one in September (76T). In addition, the reported number of virus in October was 1,210: 6.9% decreased from 1,301 in September.

(*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 October, the reported number was 1,210 and the aggregated virus count was about 70T.

The worst detection number was W32/Netsky with about 59T: W32/Mydoom with about 3.3T and W32/Mytob with about 2.8T followed.

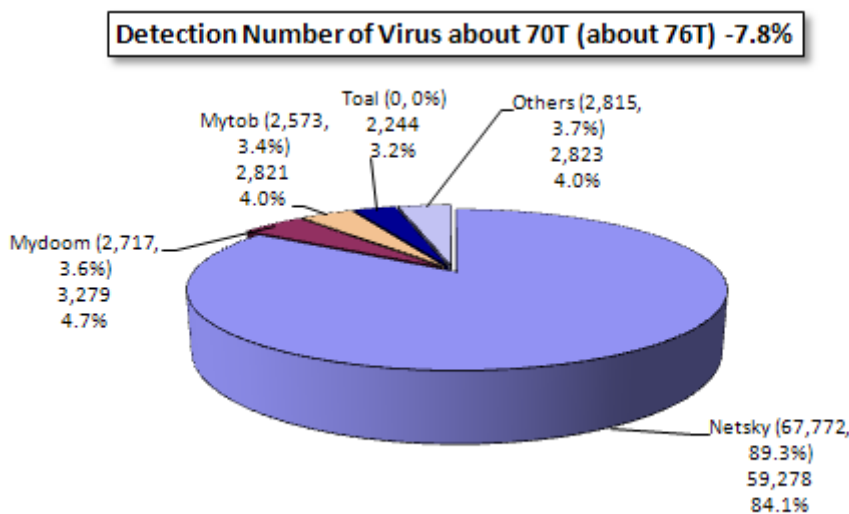


Chart 2-1: Detection Number of Virus

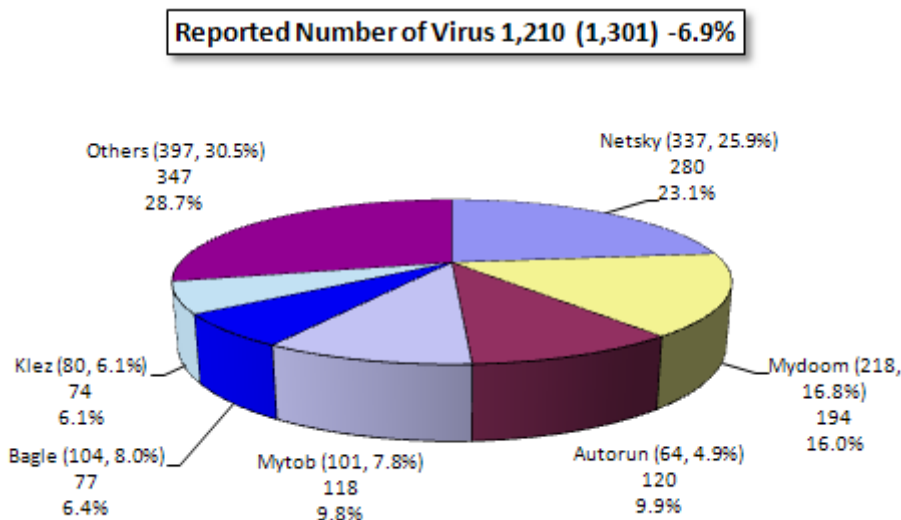


Chart 2-2: Reported Number of Virus

(2) Detection Status of the Falsified Program

In September 2009, the detection number of the “falsified security measures software” type of virus was drastically increased (see the Chart 2-3). As we specifically parsed in the introductory chapter followed by the “1. Reminder for the Month”, this may be the cause that the mails to which FAKEAV appended were massively distributed to infect the “falsified security measures software” type of virus. When infected, it usually causes significant damages: in the worst case, you need to initialize your computer to recover from the infection: Accordingly, as always, you are to be cautious with the information about the virus continually.

For your further information, number of such falsified programs having been distributed as the attachment file to e-mail: as you will see it from the Chart 2-3 below, they move artificially as they significantly increase at certain period of time, etc. This may be the cause that massive mails are concurrently distributed by bot, etc.

At the Cyber Clean Center (CCC), they are providing anti-bot measures as well as its removable tools on their web site. Be sure to utilize them as the part of infection prevention measures to check with or without of bot and/or to block installing falsified program in your computer, etc.

<Reference>

“The knowledge how to prevent infection” (Cyber Clean Center) (in Japanese)
<https://www.ccc.go.jp/knowledge/>

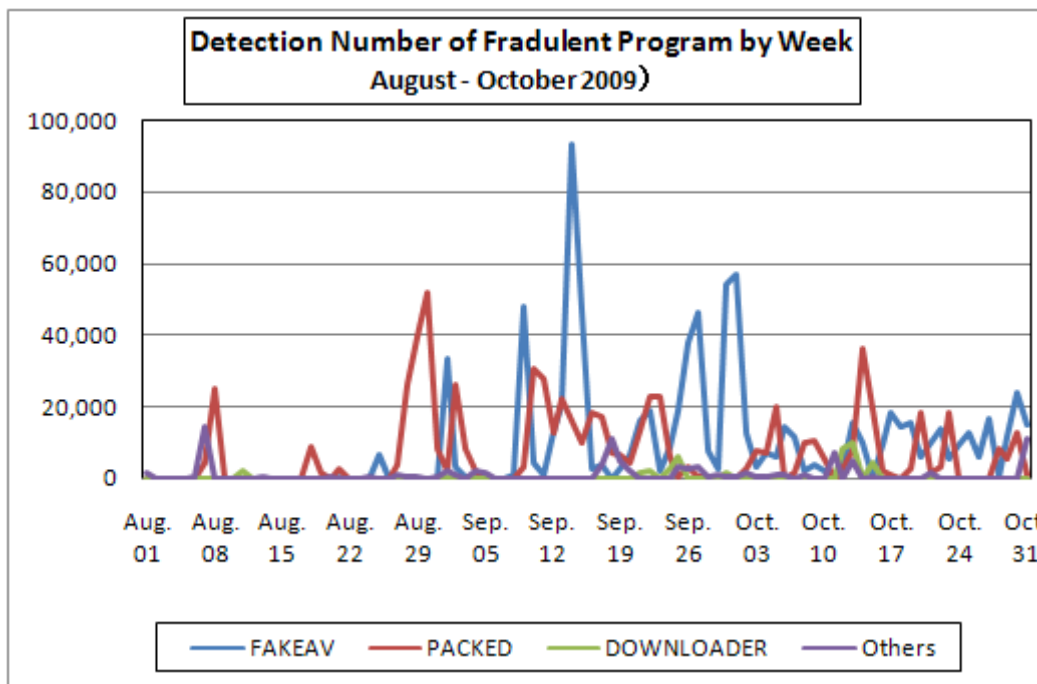


Chart 2-3: Detection Number of Falsified Program/Type by Month

III. Reporting Status of Unauthorized Computer Access (includes Consultations) –

Please refer to the Attachment 2 for further details –

Chart 3-1: Reported Number for unauthorized computer access and the status of consultation

| | May | June | July | Aug. | Sep. | Oct. |
|-----------------------------------|-----------|-----------|-----------|-----------|-----------|-----------|
| Total for Reported (a) | 8 | 7 | 14 | 20 | 11 | 21 |
| Damaged (b) | 6 | 6 | 6 | 12 | 8 | 14 |
| Not Damaged (c) | 2 | 1 | 8 | 8 | 3 | 7 |
| Total for Consultation (d) | 45 | 35 | 24 | 39 | 44 | 34 |
| Damaged (e) | 16 | 9 | 3 | 17 | 13 | 11 |
| Not Damaged (f) | 29 | 26 | 21 | 22 | 31 | 23 |
| Grand Total (a + d) | 53 | 42 | 38 | 59 | 55 | 55 |
| Damaged (b + e) | 22 | 15 | 9 | 29 | 21 | 25 |
| Not Damaged (c + f) | 31 | 27 | 29 | 30 | 34 | 30 |

(1) Reporting Status for Unauthorized Computer Access

Reported number in October was **21**: Of **14** was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was **34** (of **4** were also counted as reported number): Of **11** was the number actually damaged.

(3) Status of Damage

The breakdown for the damage reports were **intrusion** with **6**, **unauthorized mail relay** with **1**, **DoS attack** with **1** and **masquerading** with **6**.

As for the damages caused by “intrusion” were: maleficent file was located and/or file was destructed on web servers with 3, servers were exploited as the steppingstone server to attack to the other sites with 2, data theft from servers with 1. The damage cause relevant to “intrusion” included: the vulnerability in web application was exploited with 3 (of 2 were the vulnerability (ies) relevant to phpMyAdmin), insufficient password management with 2 and insufficient configuration with 1.

As for the damages caused by “masquerading”, someone spoofing to be the legitimate user for on-line services logged in and used the services without asking with 6 (i.e., on-line games with 5 and shopping portal with 1) was the major cause.

(4) Damage Instance

[Intrusion]

(i) Vulnerability in web applications was exploited and intruded to locate maleficent file (s) ...

| | |
|----------|---|
| Instance | <ul style="list-style-type: none">- Had developed some text files which we do not know was located on the server which operates Geeklog, the one of open source CMS (Contents Management System).- "Hacked by S.W.A.T" written on the text file could be read.- Study was conducted: it was realized that the vulnerability in another application so called FCKeditor which appended to Geeklog was attacked and the server was exploited/intruded.- Accordingly, we immediately up-date the FCKeditor to the latest version. |
|----------|---|

(ii) Fraudulent program was embedded so that the server was exploited as the steppingstone server to attack to other site (s) ...

| | |
|----------|---|
| Instance | <ul style="list-style-type: none">- "We monitor number of suspicious accesses from the server you are managing." so communicated from the outside of the organization.- Upon studied, it was realized that there located fraudulent program, etc. which probing vulnerability in the other computers on one server and was on operation. As its results, the server was turned to be the steppingstone server to attack to the other sites.- The cause was that the password for one account registered on that server was analyzed and intruded.- The password had never been changed when it was initially created by the owner who manages the account so that it was easily assumable. |
|----------|---|

IV. Accepting Status of Consultation

The gross number of consultation in October was 2,049. Of the consultation relevant to “**One-click Billing Fraud**” was **793** (September: 650) and was marked the worst figure ever before. The consultation relevant to “**Hard selling of falsified anti-virus software**” was **6** (September: 6), the consultation relevant to “**Winyy**” with **3** (September: 0), were also realized. (The consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” was **0** (September: 0).

Table 4-1: Gross Consultation Number Accepted by IPA over the Past 6 Months

| | May | June | July | August | Sept. | Oct. |
|---------------------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Total | 1,765 | 1,898 | 1,708 | 1,792 | 1,653 | 2,049 |
| Automatic Response System | 992 | 1,081 | 923 | 1,015 | 915 | 1,157 |
| Telephone | 710 | 777 | 736 | 702 | 676 | 843 |
| e-mail | 58 | 37 | 47 | 68 | 60 | 45 |
| Fax, Others | 5 | 3 | 2 | 7 | 2 | 4 |

*IPA consults/advises about computer viruses, unauthorized computer accesses, problems relevant to Winyy 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, winyy119@ipa.go.jp for emergent consultation relevant to Winyy, 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. Reporting Status of Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

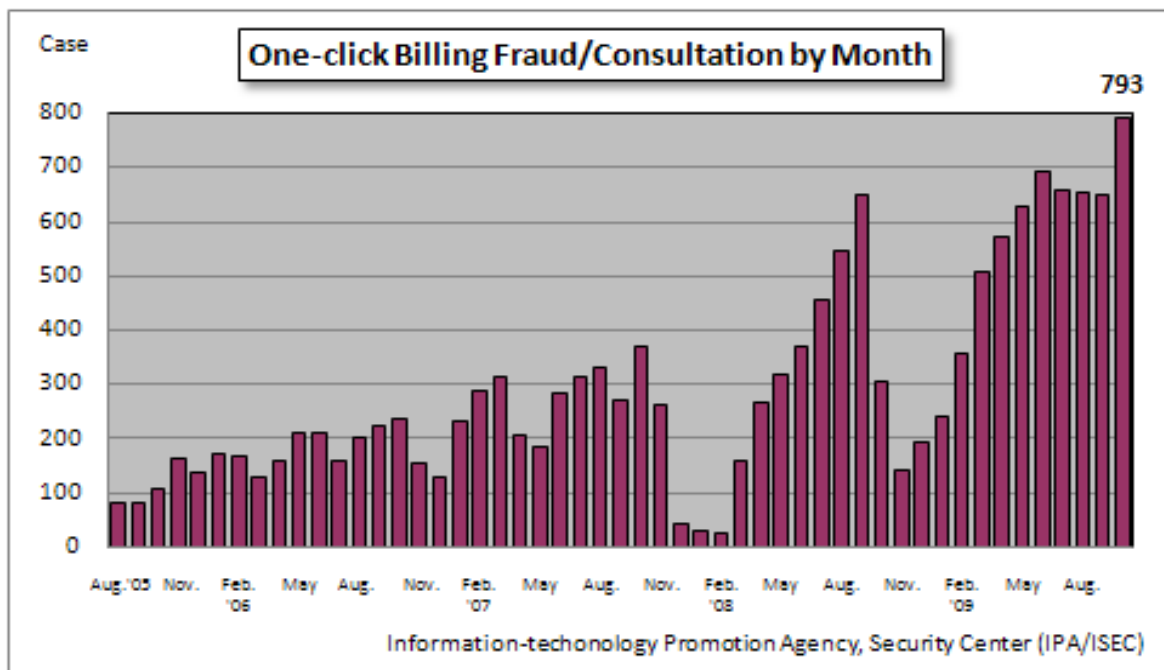


Chart 4-1: One-click Billing Fraud/Consultation by Month

The major consultation instances are as follows.

- (i) When I sneaked to browse an adult site with the computer in my office, the billing statement on my display is remained to stay with my possible effort...?

| | |
|----------------------------|---|
| <p>Consultation</p> | <p>I sneaked to browse an adult site with the computer in my office. Since it came to my ears that users can watch adult movies free of charge, I went down by clicking buttons appeared on my display in turn; then a billing statement which followed by the message saying “Your registration has successfully completed” could not be disappeared. I inquired it to IPA and realized that my computer is infected by virus. The consultant kindly advised me how to address it; an error message with “Administrative privilege is required” is displayed and is far beyond of my account. Though I attempted to log in with one of administrative account, I am totally unable to address it.</p> <p>(Other than this, we’d filed more than 10 cases of similar troubles when reporters browsed an adult site with the computer in their office.)</p> |
| <p>Response</p> | <p>With the computers in an office to which “restrictive account” have been configured, there may be difficulties upon restoring them. It is possible to configure certain administrative privilege on your account tentatively to address such troubles; however, you need to give reasonable excuses to the system administrator in your office.</p> <p>Fundamentally, browsing an adult site in your office is allowed? It may be varied from business to business, but most of them probably provide certain disciplines. Other than adult sites, there are number of malicious sites that attempt to infect users’ computers in the cyber world. It depends, but there is such virus which enlarges infection to the other users in your office. Accordingly, if you will be the casualty, your responsibility is significant, indeed. Be sure to refrain browsing such site (s) which is not directly related to your work during office hours.</p> <p><Reference></p> <p>IPA – “[Information calling for attention] Consultation relevant to one-click billing fraud is significantly increased!” (in Japanese)</p> <p>http://www.ipa.go.jp/security/topics/alert20080909.html</p> |

- (ii) Of some 10s of computers in my office were infected by virus...?

| | |
|----------------------------|---|
| <p>Consultation</p> | <p>One personnel traveled overseas: he/she stored data obtained there in an USB memory and got back to Japan. Upon inserted the USB memory to his/her computer to retrieve the data, the computer gets anomaly behaving. In the mean time, some servers that are operated in my office also anomaly behaves. Further, of about 50 computers in my office behave differently. Their symptoms are as follows:</p> <ul style="list-style-type: none"> -Unable to input Japanese. -There is a file (s) which seems to be the icon for a folder, but has .exe extension on the server. -Since virus was detected with anti-virus software and was removed; however, such configuration “Showing user the file extension” is unchangeably turned to be disabled. |
| <p>Response</p> | <p>Of some of the USB memory infection type of virus, there is such virus which enlarges infection by copying itself to the network sharing folder, or by exploiting vulnerability in the other computers (MS08-067); it seems that the virus is spread over in your office.</p> <p>Further, it seems that the computers may have been infected by the newly</p> |

emerged viruses as well for which virus signature has not yet been available. Because number of computers in your office is already infected by virus and the newly emerged virus (es?) as well, asking security professionals is the shortcut for earlier resolution.

<Reference>

IPA – Reminder for April 2009 “Are you always recognizing security measures for USB memory?”

http://www.ipa.go.jp/security/english/virus/press/200904/E_PR200904.html

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in October was **161,716** for the 10 monitoring points and the gross number of source* was **66,430**. That is, the number of access was **522** from **214** source addresses/monitoring point/day.

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

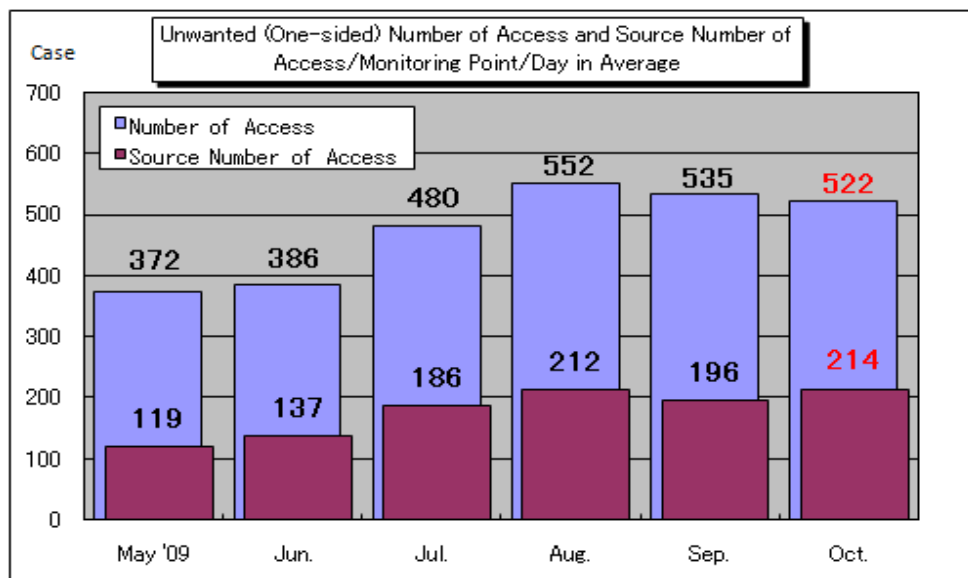


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day in average from May to October 2009. Both unwanted (one-sided) number of accesses were subtly decreased from the ones in September.

The Chart 5-2 shows the comparison in number of access classified by destination (by port) in September and October. As the graph shows, the access to the port 445/tcp was increased about 40% from the one in September.

The port 445/tcp is one of the renowned ports to be targeted by the viruses and worms which exploit vulnerability (MS08-067) in Windows. The vulnerability (MS09-050) in SMB(*)v2 in Windows publicized by Microsoft on October 13, 2009 (U.S.time) was also relevant to the port 445/tcp.

In TALOT2, such access increase to the port 445/tcp had been monitored on and around the vulnerability information was publicized, there may have been some malicious activities which attempted to exploit this vulnerability (see the Chart 5-3). Since this vulnerability can be permanently addressed by applying the modification program which provided by Microsoft on the day the vulnerability was publicized: accordingly, be sure to apply it immediately for your further security.

(*) SMB is referred as Server Message Block. This is the one of file sharing protocols to be used by the computer on Windows by default. SMBv2 (SMB Version 2.0) is the up-dated version for the default SMB and

only supported by Windows Server 2008, Windows 7 and Windows Vista.

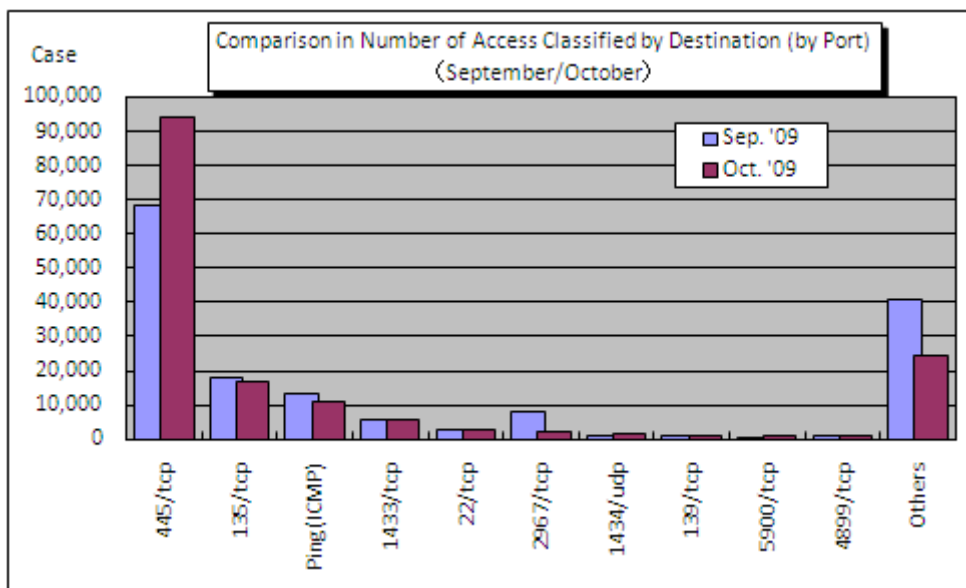


Chart 5-2: Comparison in Number of Access Classified by Destination (by Port) (September: October)

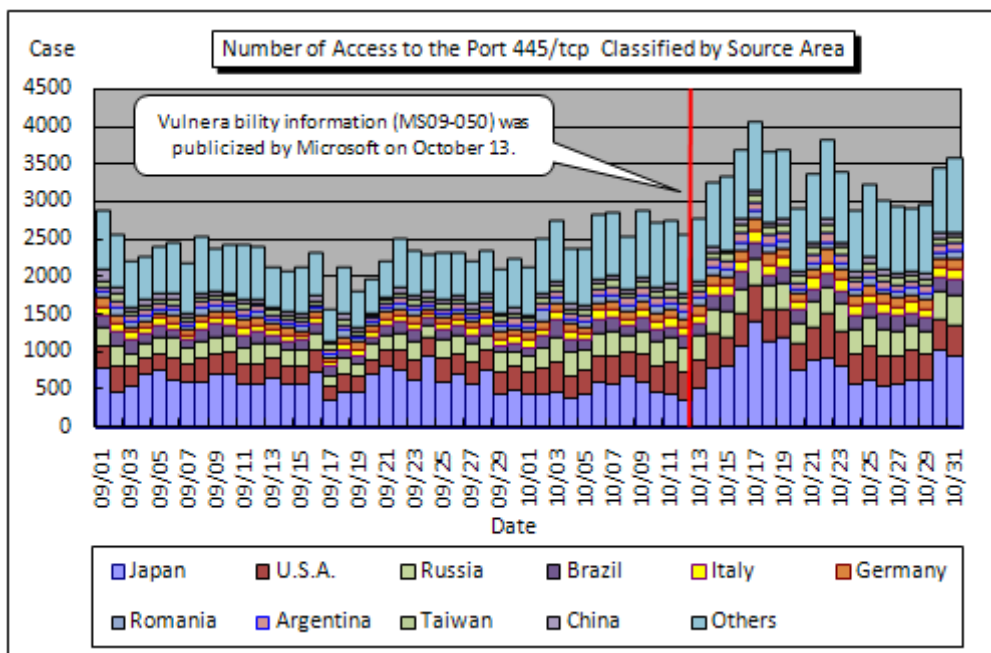


Chart 5-3: Number of Access to the Port 445/tcp Classified by Source Area (10 Monitoring Points Total)

<Reference>

“Vulnerabilities in SMB could allow remote code execution” (Microsoft)
<http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx>

“Information relevant to the vulnerability (MS09-050) in MSBv2 in Microsoft Windows” (IPA)
<http://www.ipa.go.jp/security/ciadr/vul/20091014-ms09-050.html>

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/TALOT2-0910.pdf>

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

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/summary0910.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/virus0910.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/2009/documents/crack0910.pdf>

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

JPCERT/Coordination Center (CC): <http://www.jpCERT.or.jp/>

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

Council of Anti-Phishing Japan: <http://www.antiphishing.jp/>

Symantec: <http://www.symantec.com/>

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