

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

This is the summary of computer virus/unauthorized computer access incident report for January 2010 compiled by IPA.

I. Reminder for the Month

- Be Sure to Know about the “Gumblar” Mechanism to Ensure Your Security! -

From the end of 2009, such news “such websites for renowned corporations and public organizations having been altered and those users who browsed the sites may have been infected by virus” was continually reported: actually, the consultations and inquiries about the news are rushed to IPA as well. The series of attacks so called “Gumblar” generally refers the one of attacking mechanisms to infect virus number of computers by combining “website alteration” activity (ies) and “drive by download virus (the virus gets to infect to a user’s computer who simply browsed a website)”.

For here, we will describe about the “Gumblar” mechanism, its negative effects and the countermeasures as well. Since “Gumblar” is the combination of various attacking methods used on the current Internet, following countermeasures also effective for the other threats other than “Gumblar”. Be sure to recognize that all the level of the Internet users is now facing such risks and to conduct sufficient countermeasures, accordingly.

(1) What is “Gumblar”?

“Gumblar” does not refer a specific virus. “Gumblar” refers the series of attacking methods to infect various virus number of computers by combining several attacking methods by a malicious intent (an attacker). Accordingly, to comprehend what the “Gumblar” is, it is necessary to know not only what role (s) the attacker, victim/casualty, virus, etc. possesses, but also know how they work together. The Chart 1-1 shows the entire attacking mechanism driven by respective “Gumblar” methods.

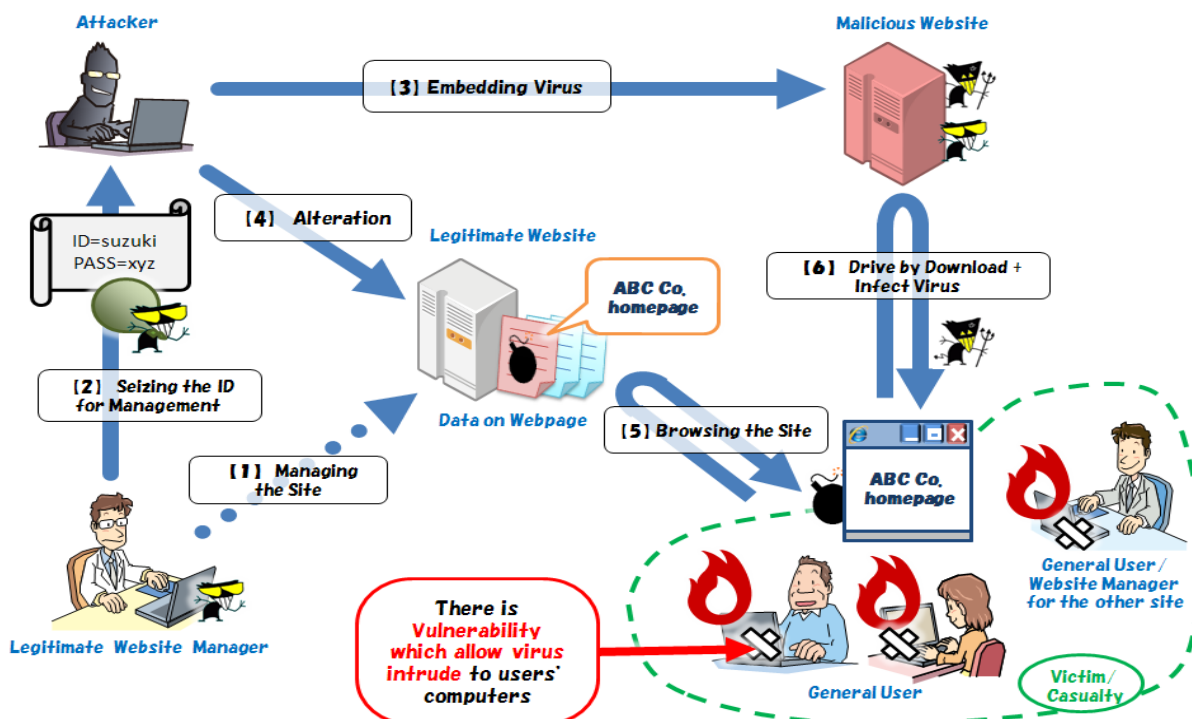


Chart 1-1: Entire Attacking Mechanism Driven by “Gumblar”

We will specifically describe them in the following sections: the major threats by the “Gumblar” that users will face are:

- With such computer for which security is not enough, the user will be infected by virus by simply browsing the website previously altered, but it may be hardly recognizable.
- Since renowned website (s) will be exploited by the “Gumblar” attack, the one of preventive measures such as “Do not browse suspicious website” does not work out and the website the user browses daily will turn to be a risky website suddenly.
- The virus which cause damage is not specified: Since the attacker can determine what virus he/she wants to infect, users cannot take specific actions to combat with.

In this way, the “Gumblar” attack will cause entire level of the Internet users. Follows, we will describe the “Gumblar” methods respectively as well as the preventive measures that the users have to take.

(2) The Specific “Gumblar” Mechanism

In this section, we will describe the “Gumblar” mechanism specifically. For your information, the mechanism is organized by several infection methods (*1) and they are further sophisticated day by day or even a minute by minute. For here, we will introduce you the typical “Gumblar” mechanism, the trend from the end of 2009. Please note if you read “【1】”, etc. in the following paragraphs, they correspond to the 【1】, etc. in the Chart 1-1 so that be sure to refer to the respective parts in the Chart 1-1 when you read.

(*1) Actually, of the mechanisms, the trend from March to May 2009, was specifically named as “Gumblar” and a different name (s) was given as the mechanism was further sophisticated thereafter. However, nowadays, those mechanisms are collectively called as “Gumblar” or the “Gumblar” variant (s).

【1】 Website Management via the Legitimate Website Manager

The 【1】 is not actually a part of the “Gumblar” mechanism, but we will describe it as its background. As you are aware that the website (s) on the Internet is managed/run by the website manager in where number of data for the web pages (i.e., display images) is stored. Upon creating/updating web pages, the website manager uses the secret ID and the password exclusively for website management so that nobody can alter/modify the web page without permission.

【2】 Seizing of the ID and the Password for the Legitimate Website Management

From 【2】 to 【4】present preparatory steps taken by a malicious intent (i.e., an attacker) as the part of the “Gumblar” mechanism. First of all, the attacker steals the ID and the password for the legitimate website from its website manager with some way. It is assumed that the virus which steals information (i.e., spyware), etc. is utilized by the attacker.

【3】 Embedding Virus (es) to Malicious Website

The attacker prepares a malicious website (*2) in where several viruses are embedded. It can be considered that the attacker can alter/update newer viruses whenever he/she wants.

(*2) Malicious website is combined by different artifices to let anti-virus software, etc. bypass its traceability.

【4】 Alteration of Legitimate Website

Lastly, the attacker masquerades to be the (legitimate) website manager by using the ID and the password for the website management stolen from the manager to fraudulently alter/modify data being stored for the web pages. More specific, the attacker traps users with the evil command (s) to redirect those users who browsed this web page to his/her malicious website (prepared by the attacker in the 【3】step above).

【5】 Browsing the Website being Altered

In the 【5】 and 【6】, we describe a user’s activity (ies) who browsed the malicious website get infected by virus.

At first, the user accesses the website (he/she believes legitimate) as usual. The browser on

the user's computer (i.e., the Internet browser) acquires the data (display images) on the subjected web page (s) and display them. In this case, the web page is being altered by the attacker in the step [4]. Since there are number of web pages, the user cannot identify of which page (s) is altered in advance. Accordingly, there displays the web page (s) seems to be the same and functions as usual before being altered/modified, but the evil commands trapped by the attacker in the web page (s) in the step [4] start to behave covertly.

[6] Redirecting to the Malicious Website (s) and Virus Infection

Subsequently, the browser will be automatically redirected (automatically linked) to the malicious website by the evil command and the first virus file will be downloaded to the user's computer.

The first virus refers "exploit code" in precise sense as its major purpose is to intrude to the user's computer by exploiting the "vulnerability which allows virus intrude to", not causes damage to the user's computer directly. The browser attempts to open the file which includes the "exploit code". If the virus file (i.e., the exploit code) is in movie file, the virus may use the other functions other than the browser's itself such as the software for movie player, etc. What if there exists "vulnerability" which allows virus intrude to the user's OS, browser, and the other application software, the vulnerability will be exploited and it allows virus to intrude to the user's computer.

Upon successfully intruded, the virus further attempts to download another virus (es) from different malicious website (s). As we already described in the [3] above, the attacker is able to alter/update newer virus whenever he/she wants, it is hardly identify what virus will be utilized.

Since such series of activities are covertly and invisibly progressed, the user hardly realizes the risk (s) he/she is facing.

▼ The "Weakness which Allows Virus Intrusion"

Though you browsed the website being altered and the activities in the step [5] and [6] above are identified, software such as OS, browser, etc. are securely designed so that they do not allow infection fundamentally. However, there is failure relevant to security which may be developed lately: this failure can be the "weakness which allows virus intrusion". In this industry, this weakness is referred as "vulnerability".

Given all the conditions – the preparatory steps from [2] to [4] by the attacker, the user's activity (browsing the website being altered) from [5] to [6] and there is "vulnerability in the user's computer" – are met, the "Gumblar" attack can be conducted.

Since there remains vulnerability in the software in the previous versions (i.e., not yet updated), it is possible that you may get infected by virus. Be sure to conduct following countermeasures to maintain your software always up-to-dated.

(3) The Cycle the Increase of the Website being Altered

In this section, we will describe the reasons why the "Gumblar" attack is enlarging and website is altered consistently.

As you can see that there is a "general user/website manager for the other site" in the victim/casualty group at the bottom of the right hand side in the Chart 1-1. He/she browses different website (s) along with the computer which manages his/her website. Assuming that the general user/website manager will be trapped as well, the attacker locates "the virus which steals the ID and the password for website management" on his/her "malicious website".

In the [2] above, we described that the attacker steals the ID and the password for website management with some way: the stealing method itself is actually a part of "Gumblar" mechanism. In this way, the attacker can masquerade to be the other website's manager to increase his/her target computers by altering subsequent websites over and over (Chart 1-2).

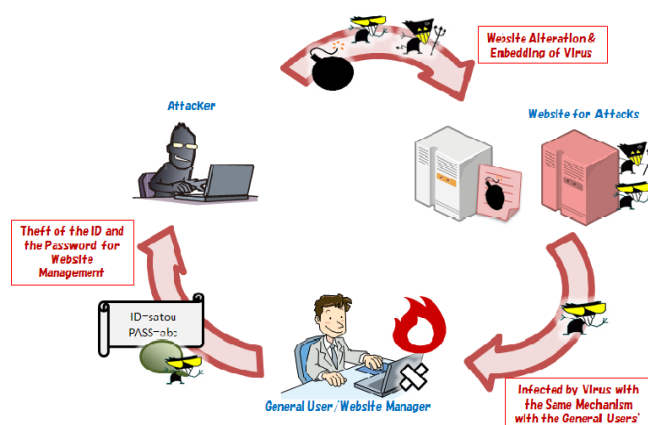


Chart 1-2: The Cycle the Attack by “Gumblar” Enlarges

▼ Summary

Follows are the summarized peculiarities of the “Gumblar” attack described in the [2] and [3] above.

- Attacker steals the ID and the password for a legitimate website management: then he/she alters the site to embed virus trap (s).
- He/she targets to those computers for which security is insufficient: then the targeted computer will be attacked with the virus which infects to the computer simply browses the website previously altered.
- The attacker again steals different ID and password for the other website’s management with the virus to increase the number of computers he/she targets.

(4) Damage Contents

As we described previously, “Gumblar” is the “mechanism to infect virus” so that we cannot presume that which virus will be used by a malicious intent and what type of damage will be expected. In addition, the virus the attacker (i.e., malicious intent) uses is also shifted as time goes by.

As of now, following virus infection via the “Gumblar” mechanism is reported to us.

- Falsified security measures software (such virus which urges to purchase a “paid-for” falsified security measures software by alerting a user fake “virus emergence”).
- The virus which steals the ID and the password (i.e., ftp account information) for (legitimate) website management.

It is hard to determine that the cause is “Gumblar”, but your computer may be infected by virus if you have following symptoms.

- Unable to run Windows Update or Microsoft Update
- Unable to link to the websites relevant to security software providers/vendors
- Unable to update the virus signature for anti-virus software

The viruses frequently distributed currently include not only those which destruct data stored in a computer, but also those which steal personal information such as the ID and the password for on-line banking/on-line games (i.e., spyware). Of some (i.e., bot) which hijacks a user’s computer to remotely manipulate, etc. are also included. Hereafter, it is probable that the “Gumblar” mechanism will be used to distribute above mentioned viruses frequently: please be cautious.

For the businesses and the managers who run own websites, they may lose their credit against those who browsed their websites if they were turned to be the victimizers who cause damage by virus infection. Accordingly, be sure to conduct sufficient countermeasures to prevent virus infection.

(5) Countermeasures

As we previously described that the “Gumblar” is not a virus itself, but the complexed mechanism to infect/distribute virus (es) to users’ computers: however, respective attacking methods used in the mechanism are not quite new. Accordingly, it is possible to prevent virus infection if you conduct fundamental countermeasures thoroughly. In this section, we will again describe about the countermeasures so that never fail to conduct them.

(i) Fixing Vulnerability

As we described in the 【6】 above, “drive by download virus” intrudes by exploiting the vulnerability, i.e., the “weakness which allows virus intrusion” within your computer. Thus, removing this vulnerability is the one of most important countermeasures.

Vulnerability (ies) may exist in OSs (such as Windows), browsers (such as the Internet Explorer), other application software, etc. respectively. As for the software installed in your computer, try to update all of them as far as possible to resolve any of vulnerabilities.

Following are the supplementary descriptions how to update your software.

- Updates for Windows (OS itself), the Internet Explorer, Microsoft Office (i.e., Word and Excel)
 - * Depends on the configuration, your computer will be updated automatically if “automatic updating” function is selected by default. If you update manually, you may use “Windows Update” or “Microsoft Update”. For their specific information, please refer to the Microsoft website below.
 - * <Reference> Microsoft Update overview
<http://www.microsoft.com/security/updates/mu.aspx>
- Check with “MyJVN Version Checker”
 - * IPA provides such tool with which you can check if such software easily targeted by virus such as Adobe Flash Player, etc. is installed in your computer and whether they are up-to-dated or not. For further information, please refer to the following “My JVN Version Checker” web page.
 - * <Reference> “My JVN Version Checker” (IPA)(in Japanese)
<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>
<As of February 2010, “My JVN Version Checker” supports Windows XP and Vista.>
- The other software
 - * How to update software may vary respectively. It is ideal to inventory software installed in your computer and to update them regularly. Though this activity is hardly conduct for a PC beginner, be sure to learn it gradually for your further security.
 - * Here in IPA, we immediately alert all the level of users in case developed vulnerability (ies) in the software the users use the most (please refer to the “List of Emergency Countermeasures/Security Alert” underneath). In case alerted, be sure to check whether the software alerted is installed in your computer: if yes, be sure to respond to it adequately.
 - * <Reference> “List of Emergency Countermeasures/Security Alert” (IPA) (in Japanese)
<http://www.ipa.go.jp/security/announce/alert.html>

(ii) Installing of Anti-virus Software

None of anti-virus software is almighty, but is the one of important countermeasures. By installing anti-virus software and maintaining its signature to be always up-to-dated, you can block virus intrusion and/or remove virus (es) already intruded. Since current virus engineering makes their infection activities hardly identifiable so that anti-virus software is the fundamental tool to detect and remove them.

As for the anti-virus software for general users, we recommend to select “integrated” type

which provide not only develop/remove virus, but also furnish such function to block user going forward to browse malicious website (s), etc. For your information, anti-virus software will be of help against the “Gumblar” mechanism in the following circumstances.

- Block the user going forward upon he/she attempts to open the website previously altered **(【5】)**
- Block the “exploit code” downloaded by a malicious website **(【6】)**
- Block the virus (es) subsequently downloaded by the “exploit code” **(【6】)**
- In case infected, it can develop/remove virus (es) at a later date.

(iii) Countermeasures against “Zero Day Attack”

Up to here, we mainly described how to resolve vulnerability (ies); however, such period that vulnerability is initially developed from till its modification program will be released, we are unable to resolve that vulnerability. The attack which specifically targets this period is called “Zero day attack”. In this period, we have to take preventive measures as possible as we can (“preventive measures” may vary greatly for the software targeted by that attack).

It is reported that there identified the “Zero day attack” as the part of the “Gumblar” mechanism. For detailed information relevant to the “Zero day attack”, please refer to the following URL.

<Reference>

“The Zero day attack which targets vulnerability for which remediation program has not provided yet” (IPA) (in Japanese)

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

(iv) Infected by Virus/ Worrying about Infection

If you are not for sure you are infected by virus or not, the considerable mean is to check/remove with anti-virus software. It is possible that your computer may be infected by unknown (i.e., newer) virus (es) which your anti-virus software cannot detect; however, the anti-virus software will respond to it (i.e., by updating the virus signature in that anti-virus software) and you may be able to define the virus (es).

In case your computer behaves anomaly and/or you are unable to detect/remove virus by your anti-virus software installed, the last resort to remove virus (es) thoroughly is to initialize your computer (return to your computer back to the initial state upon you’d purchased).

As we repeatedly described, the preventive measures from (i) to (iii) is further important than the handling of the computer already infected.

(v) Countermeasures as a Website Manager

There are several considerable countermeasures to be taken by a website manager other than the countermeasures mentioned above. You will be able to refer them by accessing following URL.

<Reference>

“For Website Managers: Security Alert relevant to Website Alteration/
For General Users: Security Alert relevant to Virus Infection by the Website Previously Altered” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/topics/20091224.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^(*1) in January was about 72T: increased about 9% from about 66T in December '09. In addition, the reported number of virus^(*2) in January was 1,154: 17.6% increased from 981 in December '09.

(*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 January, the reported number was 1,154 and the aggregated virus count was about 72T.

The worst detection number was for W32/Netsky with about 46T: W32/Waledac with about 8.4T and W32/Mumu with about 7.5T respectively followed.

Detection Number of Virus about 72T (about 66T) +9%

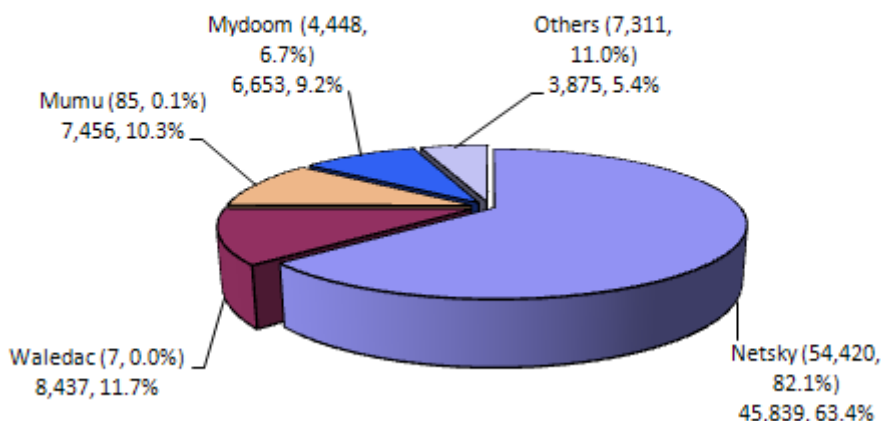


Chart 2-1: Detection Number of Virus

Reported Number of Virus 1,154 (981) +17.6%

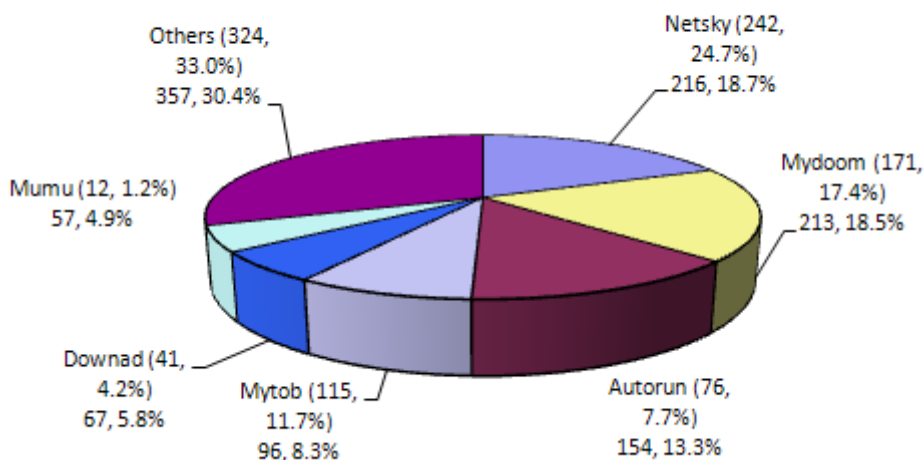


Chart 2-2: Reported Number of Virus

(2) Detection Status of Falsified Program

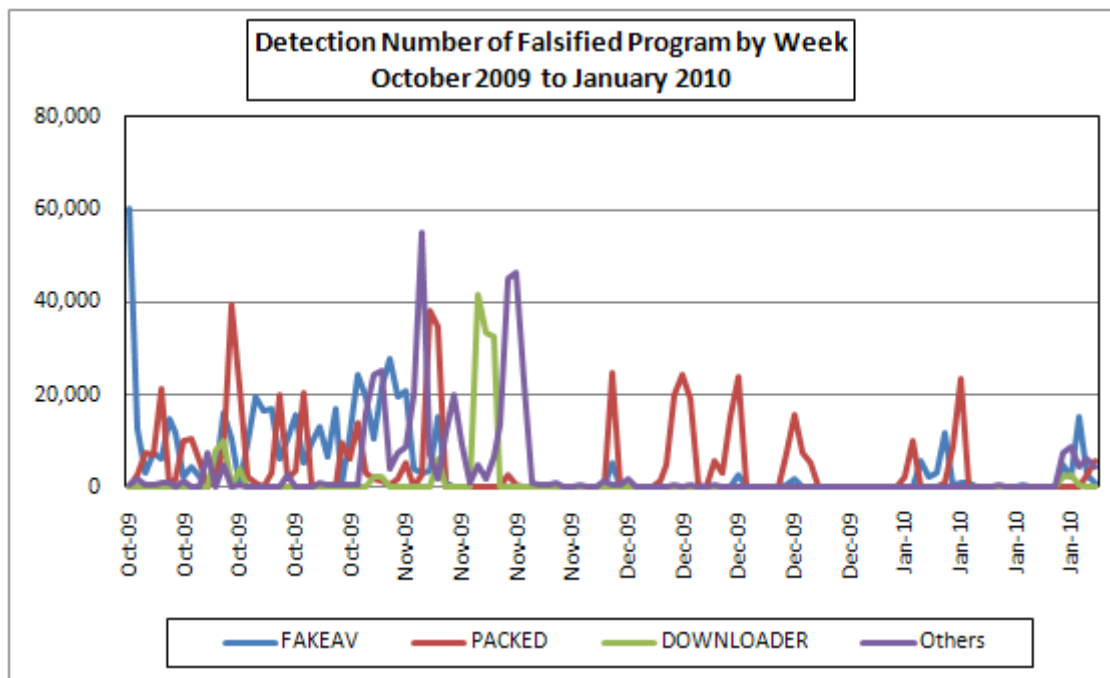
The detection number of fraudulent program such as “falsified security software” type of virus (FAKEAV), etc. tends to decreasing entirely (See the Chart 2-3).

Number of such fraudulent program is distributed as the attachment file to e-mail: as you can see in the Chart 2-3 below, they behaves artificially as they drastically increase/decrease at certain period of time. It is assumed that this may cause that the number of mails was distributed concurrently by bot, etc. so that we have to be cautious as we cannot presume when they will be drastically increased. We identified that the detection number was significantly increased at several days in January.

In the Cyber Clean Center (CCC), they provide anti-bot measures as well as their removal tools. To NOT being a victimizer who distribute virus while you do not know, be sure to conduct adequate security measures to prevent infection by bot: ensuring that your computer is free from bot virus and/or never, ever downloading falsified program is essential.

<Reference>

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



2-3: Detection Number of Falsified Program by Week

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

	Aug. '09	Sep.	Oct.	Nov.	Dec.	Jan.
Total for Reported ^(a)	20	11	21	11	9	20
Damaged ^(b)	12	8	14	6	6	12
Not Damaged ^(c)	8	3	7	5	3	8
Total for Consultation ^(d)	39	44	34	34	22	67
Damaged ^(e)	17	13	11	14	14	34
Not Damaged ^(f)	22	31	23	20	8	33
Grand Total ^(a + d)	59	55	55	45	31	87
Damaged ^(b + e)	29	21	25	20	20	46
Not Damaged ^(c + f)	30	34	30	25	11	41

(1) Reporting Status for Unauthorized Computer Access

Reported number in January was **20**: Of **12** was the number actually damaged.

(2) Accepting Status for Consultation relevant to Unauthorized Access

The consultation number relevant to unauthorized computer access was **67** (of **8** were also counted as reported number): Of **34** was the number actually damaged.

(3) Status of Damage

The breakdown of damage reports were **intrusion** with **11** and **masquerading** with **1**.

The damages relevant to “intrusion” include insertion of evil codes on web pages with 9, locating fraudulent program within a web server to attack/probe the other site (s) with 2. The causes for intrusion were: the computer for web page management was infected by virus via the “Gumblar” mechanism and the ftp account information for updating the website was stolen with 1, though the details has not yet identified, it may resulted by the “Gumblar” mechanism with 8 and insufficient ID/password management with 1 (the cause for the rest of 1 has not yet identified).

As for the damage relevant to “masquerading”, someone spoofed to be the legitimate user who actually signed up with the on-line game fraudulently logged-in to the site to use the services without permission with 1.

(4) Damage Instance

[Intrusion]

(i) Evil code was Inserted to Website by “Gumblar” Attack ...

Instance	<ul style="list-style-type: none"> - Upon browsed the website run by my business located in an outside rental server, I was alerted virus. Upon browsed our blog site located in the other rental server, again, I was alerted virus. We totally relied on their management to identical home page producing company. - Study was conducted. Then it was realized that there embedded some scripts within that web page which drive user to a malicious site. Those files that have “index” within their names (i.e., index.html, index.php, etc.) and JavaScript external file (ex. Xxx.js) were altered. - The other web server managed/run within my business was not altered as accesses to edit/update the site were restricted by IP address. - It is assumed that the computer for the home page producing company was infected by virus and their ftp account information was stolen: however, the sauce computer and the virus actually caused damage have not yet identified.
----------	---

(ii) Exploited as the Steppingstone Server to Probe to the other Site (s)...

Instance	<ul style="list-style-type: none"> - “Your server attempts to access fraudulently to the other site (s) with ftp commands” so communicated by the ISP we are signing up with. - When we studied applicable server, it was realized that there embedded “FTP Scanner” and was exploited as the steppingstone server to collect to the IP address information from ftp accessible site (s). - The one of the causes was that the access was not restricted with the server as it was run by a test environment.
----------	--

IV. Accepting Status of Consultation

The gross number of consultation in January was **2,150**. Of the consultation relevant to “**One-click Billing Fraud**” was **638** (December ‘09: 576). The consultation relevant to “**Hard selling of falsified anti-virus software**” with **37** (December ‘09: 7), the consultation relevant to “**Winy**” with **1** (December ‘09: 6), the consultation relevant to “**the suspicious mail sent to specific organization to collect specific information/data**” with **0** (December ‘09: 1), etc.

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

	August	Sept.	Oct.	Nov.	Dec. '09	Jan.
Total	1,792	1,653	2,049	2,315	1,794	2,150
Automatic Response System	1,015	915	1,157	1,340	1,138	1,160
Telephone	702	676	843	918	602	910
e-mail	68	60	45	53	52	78
Fax, Others	7	2	4	4	2	2

*IPA consults/advises about computer viruses, unauthorized computer accesses, problems relevant to Winy 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, winy119@ipa.go.jp for emergent consultation relevant to Winy, 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 ⁽⁴⁾ column of the Chart in the “III. Reporting Status of Unauthorized Computer Access” and “IV. Accepting Status of Consultation”.

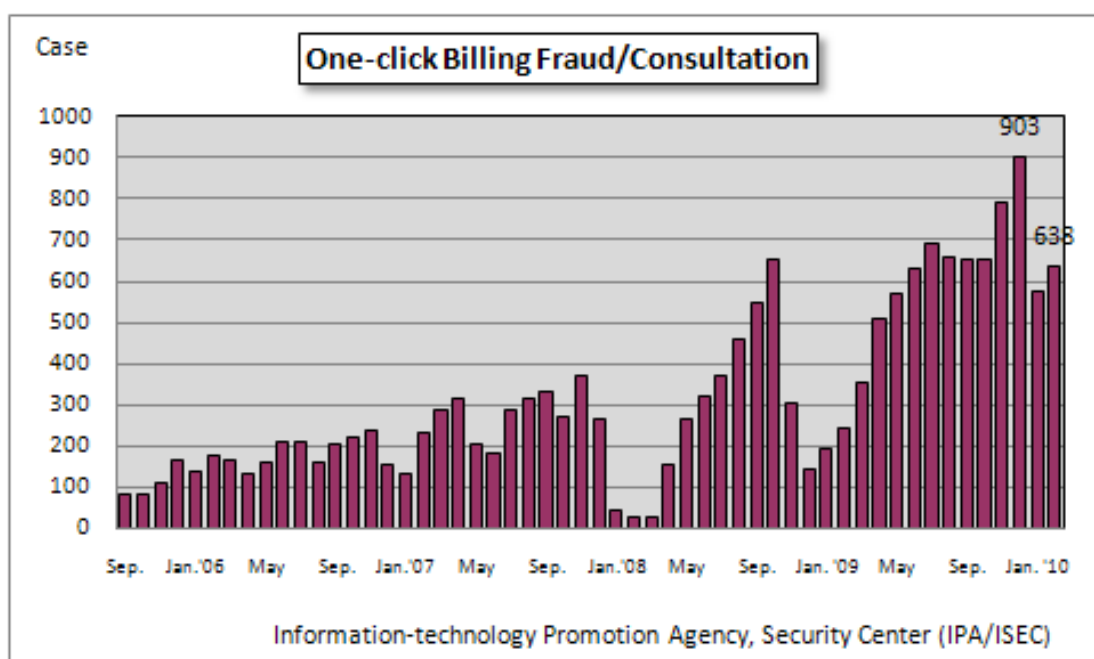


Chart 4-1: One-click Billing Fraud/Consultation

The major consultation instances are as follows.

(i) “Your computer is infected by virus!” so alerted in English ...?

<p>Consultation</p>	<p>When I booted up my computer, the software so called “Security Tool” was automatically run. It said “Your computer is infected by virus. To remove the virus, you need to install PAID-FOR anti-virus software.” Then, I was urged to input my credit card number, but I am disregarding it as I felt it suspicious. However, while I am browsing websites, the Internet is suddenly disconnected, the another anti-virus software I purchased thereafter does not work well: even I cannot restore back my system as the “Security Tool” alerts that any files cannot be opened as my computer is infected by virus so that I am blocked any of security relevant activities by this “Security Tool”. I am wondering that I am infected by virus!? I used to browse news or fortune-telling sites, but suspicious websites.</p>
<p>Response</p>	<p>“Security Tool” is the one of “falsified security measures software” type of virus. As with this instance, in current “Gumblar” mechanism, it is possible that such falsified security measures software may be automatically embedded by malicious intent. Once infected, any of restoration activities can be interrupted by the virus so that the user has to initialize his/her computer as the last resort.</p> <p>To prevent from such worst case, it is fundamental to install (legitimate) anti-virus software and maintain it always up-to-dated. It is also important to resolve vulnerability (ies) via Windows Update, etc. As for major applications that easily targeted by virus, IPA is now providing such tool which automatically checks your versions so why don’t you leverage it for your further security.</p> <p><Reference> “MyJVN Version Checker” released (IPA) http://www.ipa.go.jp/security/english/vuln/200911_myjvn_vc_en.html</p>

(ii) I wish to check/ensure my website is not altered ...?

<p>Consultation</p>	<p>I am running private homepage. Since I can frequently hear and see the news that the websites for renowned businesses are altered by “Gumblar” over and over so that I am afraid of. I’d heard that it is necessary to check all the pages: it must be toil as there are number of pages and I am not enough familiar with the HTML files. Can you suggest me of any means that I can check them easily?</p>
<p>Response</p>	<p>Just simplified methods, but there are several ways to check with.</p> <ul style="list-style-type: none"> - Check if the letter string such as “/*GNU GPL*/”, “/*LGPL*/”, “/*Exception*/”, “/g, ‘8008’, etc. is included in your HTML files (it is possible that there emerge another letter string (i.e., keyword)). - Copy all the web pages on your website to your handy computer and then check with or without virus with your <u>updated</u> virus signature (better to use different software if possible). You may also leverage free-online-scan. <p>If detected one of the said letter strings or some virus is alerted, it is possible that your website is altered. In that case, be sure to cease to publicize your homepage and take necessary actions immediately.</p> <p>Be sure to maintain those copied files for which security is ensured near you to get ready for exchange in case something would be happened again.</p> <p><Reference> “For Website Managers: Security Alert relevant to Website Alteration/ For General Users: Security Alert relevant to Virus Infection by the Website Previously Altered” (IPA)(in Japanese) http://www.ipa.go.jp/security/topics/20091224.html</p>

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

According to the Internet Monitoring (TALOT2), the total of unwanted (one-sided) number of access in January was **185,488** for the 10 monitoring points and the gross number of source* was **78,209**. That is, the number of access was **598** from **252** 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.

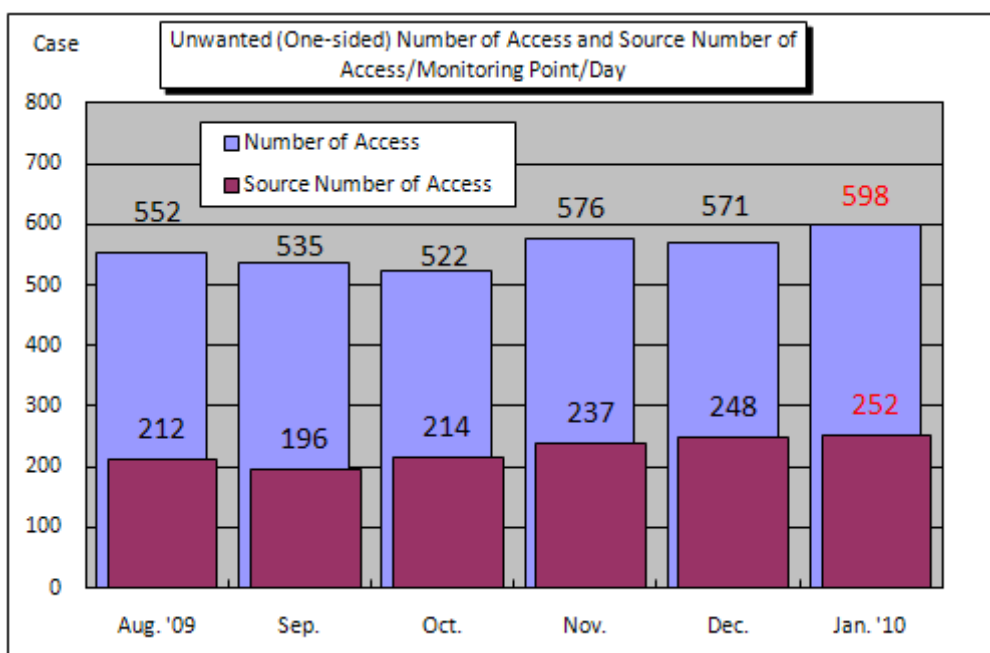


Chart 5-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day in Average

The Chart 5-1 shows the unwanted (one-sided) number of access and source number of access/monitoring point/day in average from August 2009 to January 2010. Both unwanted (one-sided) number of access and source number of access were increased from December 2009.

The Chart 5-2 shows the comparison of number of access classified by destination (by port) for December 2009 and January 2010. According to this chart, accesses to the port 445/tcp was increased, but the accesses to the other ports were shifted with the same level from December 2009.

In the TALOT2 monitoring environment, accesses to the port 445/tcp are remarkably many than the other ports; it is necessary to watch over as this port is still easily targeted by malicious intents.

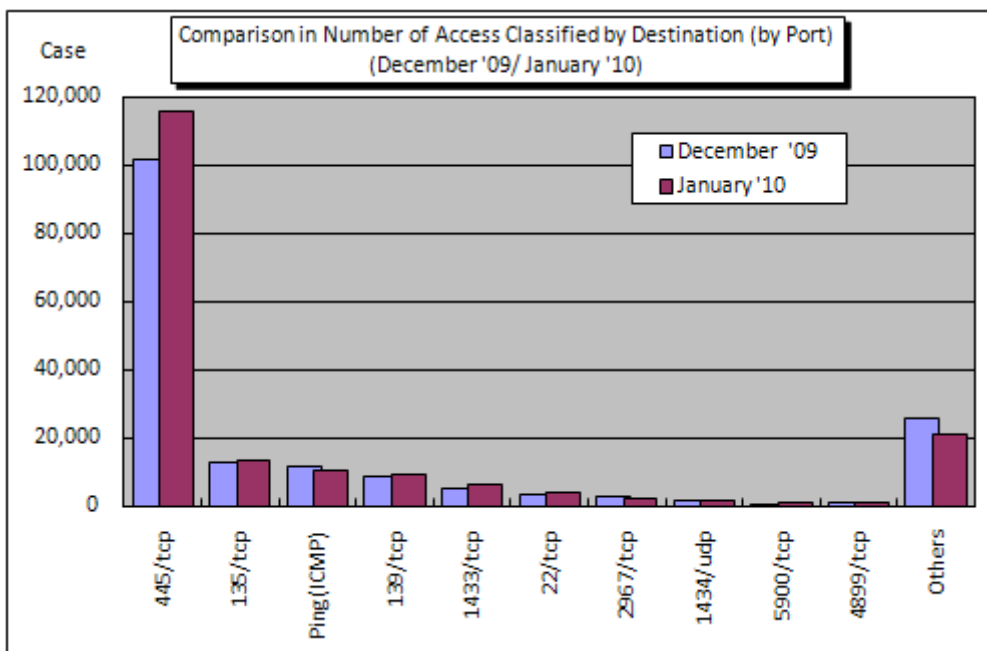


Chart 5-2: Comparison in Number of Access Classified by Destination (December '09/January '10)

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/201001/documents/TALOT2-1001.pdf>

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

<http://www.ipa.go.jp/security/english/virus/press/201001/documents/summary1001.pdf>

Attachment_1 Computer Virus Incident Report

<http://www.ipa.go.jp/security/english/virus/press/201001/documents/virus1001.pdf>

Attachment_2 Unauthorized Computer Access Incident Report

<http://www.ipa.go.jp/security/english/virus/press/201001/documents/crack1001.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