1. Computer Virus Reported

(1) General Overview for the Year 2012

The number of the cases reported for computer viruses*[1] for the year 2012 has decreased from the number for the year 2011 (see Figure 1-1). By virus type, **W32/Mydoom** was reported most. As for **XM/Mailcab** which is a type of macro virus, the number of the cases reported has been increasing gradually since such report was submitted for the first time in April 2012 (See Figure 1-2). As of December 2012, the number for this virus is showing a decreasing trend, but we need to watch out for its infection activities for a while.

As for the number of the viruses detected*[2] throughout the year 2012, **W32/Mydoom** has accounted for over half of the total, showing an increasing trend (See Figure 1-3). On the contrary, **W32/Netsky** has shown a decreasing trend throughout the year 2012, outpaced by **W32/Mydoom** in terms of both the number of the cases reported and the number of the viruses detected. But still, it has accounted for a little less than one-third of the total. **W32/Mydoom and W32/Netsky attach copies of themselves to an e-mail attachment, with the goal of spreading infection to the recipients of such e-mail. It is assumed that there are still a large number of the servers and PCs that are infected with these viruses.**

In January 2012, the number of the viruses detected for **W32/Downad** was extremely large, but they were detected only at certain enterprises. W32/Downad carries out infection activities by exploiting Windows vulnerabilities and therefore, it can be used as a foothold for carrying out "Targeted Attack". However, it can be detected by antivirus software.

As shown in Figure 1-3, the total number of the viruses detected in April 2012 was small. This was due to the fact that the number of the cases reported was also small.

In November 2012, the total number of the viruses detected for **W32/IRCbot** increased on a temporary basis. This virus was also detected only at certain enterprises. W32/IRCbot also carries out infection activities by exploiting Windows vulnerabilities or vulnerabilities within programs and therefore, it is possible that this virus was used as a foothold for carrying out "Targeted Attack" (as shown in January).

As for the number of the malicious programs detected*[3] throughout the year 2012, **Trojan/Horse**, which masquerades primarily as legitimate software and infects PCs, **Bancos**, which steals IDs/Passwords for Internet banking, and **Fakeav**, which is a collective term for fake security software, were detected in large numbers (see Figure 1-4).

As shown in Figure 1-4, the total number of the viruses detected in April 2012 was small. This was due to the fact that the number of the cases reported was also small.

The reason why the number for Trojan/Horse in May 2012 was large was because, the reports concerning this malicious program were submitted not in April but in May (NB: the number of the viruses detected is based on the report submission date.)

The reason why the total number of the viruses detected in July 2012 was large was because, Adware and Bancos were sent to certain enterprises.

In September 2012, the number for Invo was large. This was also due to the fact that it was sent in large numbers to certain enterprises.

From the number of the viruses detected and the number of the malicious programs detected, we can see that many of them reached a point within an inch of their target PCs. **However, because the users of those PC were using antivirus software, they were able to prevent their infection.**

*1 Number of the cases reported: If multiple reports submitted by the same person contained the same virus with the same detection date, they are counted as one report regarding that specific virus.

*2 Number of the viruses detected: indicates how many viruses were detected according to the reports submitted.

*3 Number of the malicious programs detected refers to the summary count of malicious programs that were reported to IPA in that period and that do not fall in the category of computer viruses defined by the "Computer Virus Countermeasures Standard".
Computer Virus Countermeasures Standard (Announcement No.952 by the Ministry of International Trade and Industry): final revision was made on Dec. 28, 2000 by the Ministry of International Trade and Industry (MITI), which was renamed the Ministry of Economy, Trade and Industry (METI) on Jan. 6, 2001.
"Computer Virus Countermeasures Standard" (METI)
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

(2) Virus Infection Cases Reported

Breakdown of the virus infection cases reported throughout the year 2012 is: **W32/Antinny** (1 case); **W32/Palevo** (1 case); **W32/Downad** (1 case); **W32/Fujacks** (1 case); **W32/Dorkbot** (3 cases); sum of which is 7 cases (see Table 1-1).

Breakdown of the infection route is: an external medium (2 cases); an e-mail (3 cases); a downloaded file (1 case); and unknown (1 case).

Breakdown of the infection cause is: downloading a file by using Winny and executing it (1 case); the antivirus software's pattern files not updated (1 case); downloading a file from a website whose URL was contained in an e-mail and executing it (3 cases); and unknown (2 cases).

Breakdown of "How it was detected" is: visual confirmation (3 cases); informed by an external party (2 cases); by installing another antivirus software and performing virus scan (1 case); and by using the antivirus software with its pattern files updated (1 case).

As for the cases reported for **W32/Dorkbot**, all the report submitters were using Skype, which is an Internet phone service and through which their PC was infected. It works in such a way that the PCs of the recipients of an e-mail whose message contain an URL are infected with it by clicking the URL and downloading and executing a certain file. If infected, an e-mail with the same message is sent to the addresses registered in the address book for Skype on that PC.

At the time a report concerning this virus was submitted for the first time, it could not be detected by most antivirus software. **So even if an e-mail was from your acquaintance, if you feel suspicious about its message, do not click or download and execute any files; instead, contact the e-mail sender (who is supposed to be your acquaintance) for authenticity and if confirmed safe, click or execute such files.**

(3) Number of Cases Reported

The number of the cases reported throughout the year 2012 was **10,351**. The graph below (Figure 1-1) shows the annual trend for the cases reported to IPA.

As shown in Figure 1-1, the number of the cases reported throughout the year 2012 decreased by **1,685** cases from the number for the year 2011 (**12,036**).

In 2012, 127 types of viruses were reported (compared to 125 in 2011); among them, 14 types were reported for the first time in 2012 (compared to 20 in 2011); meanwhile, five of them were PDA viruses (compared to 7 in 2011) that are designed to infect AndroidOS.

Breakdown of the 127 types is: Windows/DOS viruses (82 types, 9,038 cases); script and macro viruses (36 types, 1,223 cases); PDA viruses (8 types, 89 cases); and Linux viruses (1 type, 1 case).

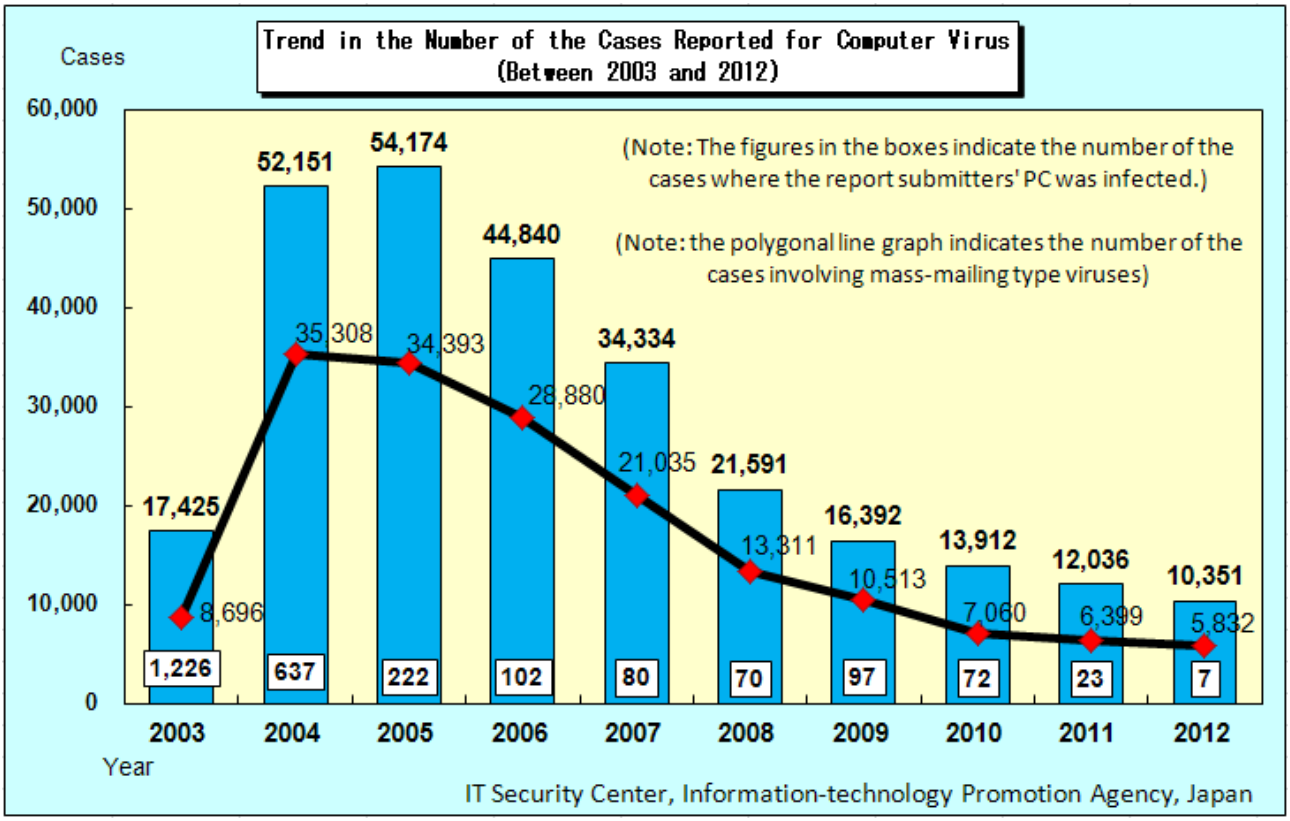


Figure 1-1: Trend in the Number of the Cases Reported for Computer Viruses (Yearly Figures)

The number of the virus infection cases reported throughout the year 2012 was: **7**. Breakdown of virus names*[4] is: **W32/Antinny (1 case)**, **W32/Palevo** (**1 case)**, **W32/Downad (1 case)**, **W32/Fujacks (1 case)**, and **W32/Dorkbot (3 cases).** The details are as follows:

Table 1-1 : Details of the Cases Reported for Virus Infection

Virus Name	Type of Report Submitter	Antivirus Software	Infection Route	Infectious Cause	How it was detected	Action taken
W32/Antinny	General corporation	Unknown	A downloaded file	An employee downloading a file by using Winny on his home PC and executing it	Informed by an external party	Disposition of that PC
W32/Palevo	Education institution	Installed (Kept up-to-date)	An external medium	Unknown	Visual confirmation	Unknown
W32/Downad	General corporation	Installed (Not kept up-to-date)	An external medium	The antivirus software's pattern files not updated	By using the antivirus software with its pattern files updated	Initialization of that PC
W32/Fujacks	General corporation	Installed (Kept up-to-date)	Unknown	Unknown	By installing another antivirus software and performing virus scan	Replacement of that antivirus software and detection and cleaning of that virus

W32/Dorkbot	Individual user	Unknown	An e-mail	Downloading a file from a website whose URL was contained in an e-mail and executing it	Visual confirmation	System restoration
W32/Dorkbot	Individual user	Installed (Kept up-to-date)	An e-mail	Downloading a file from a website whose URL was contained in an e-mail and executing it	Informed by an external party	Deletion of the executed file
W32/Dorkbot	General corporation	Installed (Kept up-to-date)	An e-mail	Downloading a file from a website whose URL was contained in an e-mail and executing it	Visual confirmation	Update of that antivirus software and cleaning of that virus

*4:For more details on the reported viruses, please refer to "The viruses that have been reported to IPA" http://www.ipa.go.jp/security/virus/virus_main.html)

(4) Number of the Cases Reported for Computer Viruses

Breakdown of the cases reported for computer viruses throughout the year 2012 is: **W32/Mydoom (2,428 cases)**, **W32/Netsky** (**1,982 cases)**, and **W32/Autorun (776 cases)** (See Figure 1-2).

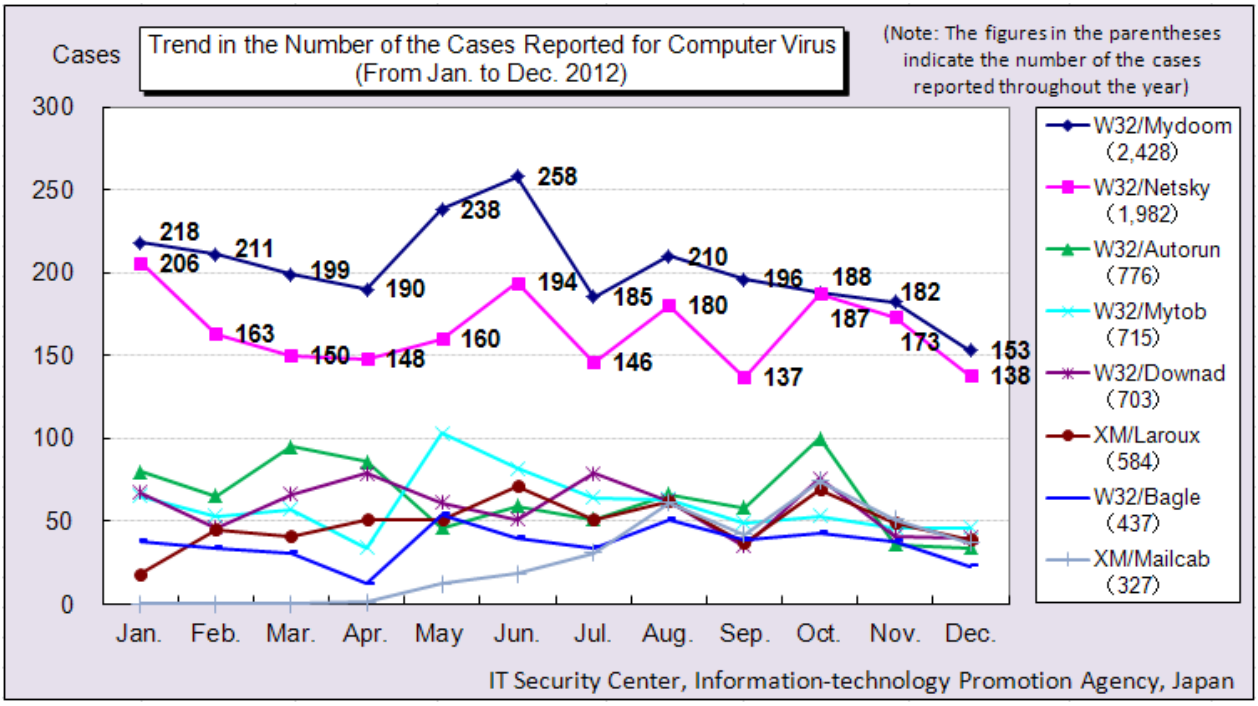


Figure 1-2: Trend in the Number of the Cases Reported for Computer Viruses (From Jan. to Dec. 2012)

(5) Number of the Viruses Detected

The number of the viruses detected throughout the year 2012 was: **249,940**, down **28,995** from **278,935** in 2011 (See Figure1-3).

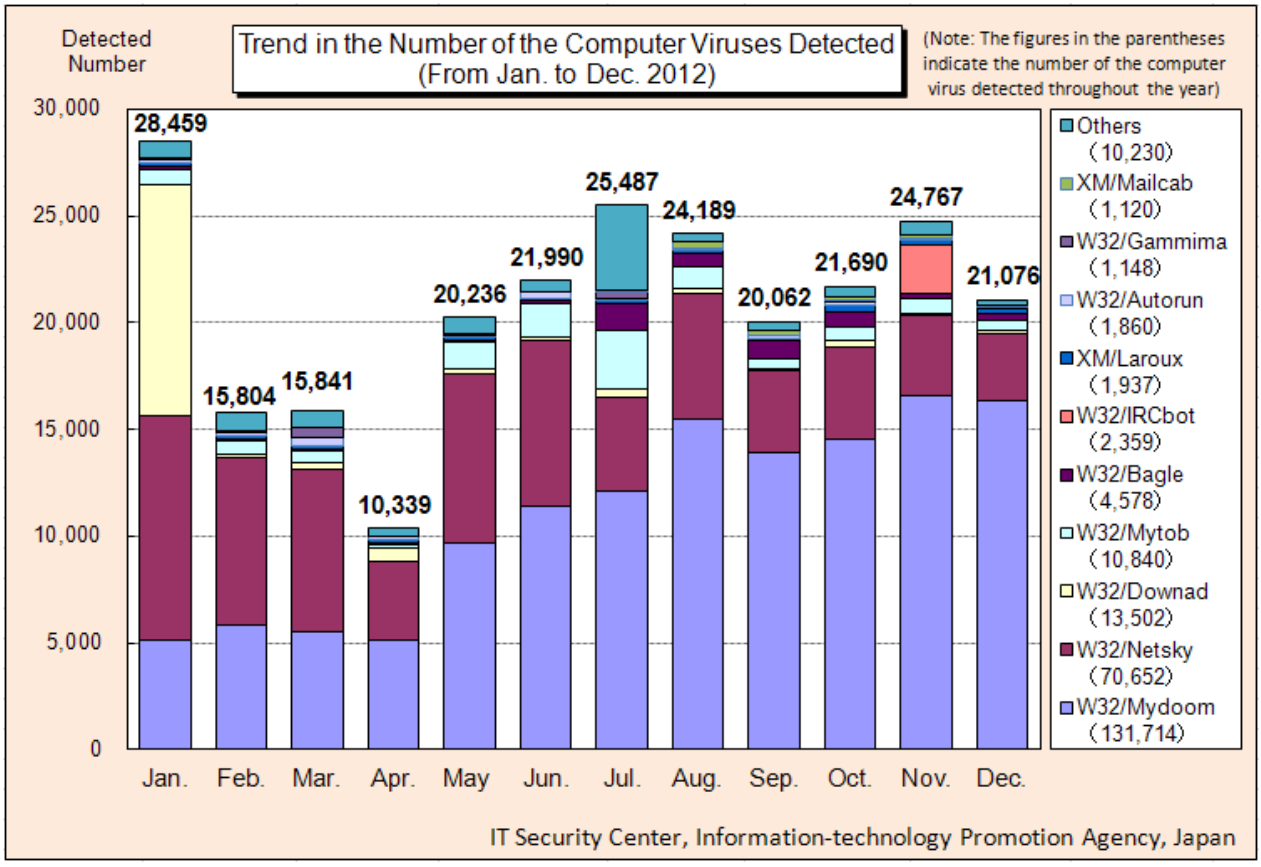


Figure 1-3: Trend in the Number of the Computer Virus Detected (From Jan. to Dec. 2012)

(6) Number of the Malicious Programs Detected

The number of the top-ten malicious programs detected throughout the year 2012 was: **230,450**, down **93,606** from **324,056** in 2011 (See Figure1-4).

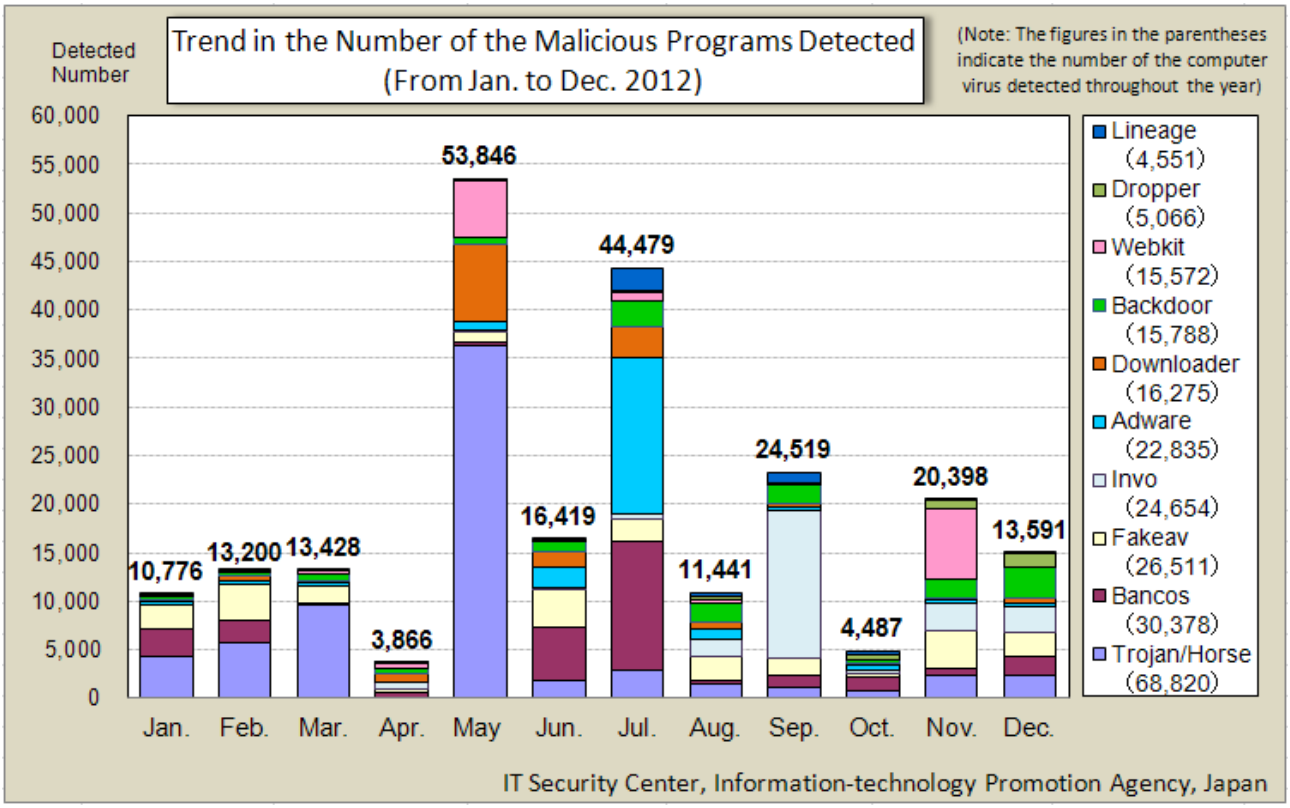


Figure 1-4：Trend in the Number of the Malicious Programs Detected (From Jan. to Dec. 2012)

Computer Virus Incident Reporting Program

This program was established and enforced in April 1990 by the Ministry of Economy, Trade and Industry (METI) according to its computer virus prevention guidelines and encourages those who detected computer viruses to report them to IPA so that the recurrence or the spread of such infection can be prevented.

While IPA responds individually to each report submitter, it also establishes countermeasures against virus incidents, based the reports submitted. Submitted reports are carefully handled to protect the privacy of report submitters and used solely for the purpose of analyzing damage situation and periodically releasing our findings.

Computer Virus Prevention Guidelines:

Established on July 7, 1995 (Ministry of International Trade and Industry (MITI) release No. 429)
Revised on September 24, 1997 (MITI release No. 535)
Final revision on December 28, 2000 (MITI release No. 952)

The One Designated by the Minister of Economy, Trade and Industry:

January 5, 2004 (METI release No. 2)

Inquiries to:
Kagaya/Aoki at IT Security Center, Information-technology Promotion Agency, Japan
Tel:03-5978-7591
E-mail:isec-info@ipa.go.jp

2. Unauthorized Computer Access Reported

(1) General Overview of the Year and Information on Countermeasures

In 2011, the number of the cases reported for a website defacement that exploits vulnerabilities within Content Management System (CMS) increased. In 2012, in addition to that, the reports on a website defacement that exploits vulnerabilities within server management tools stood out. Since the most of the causes of damages were unknown, we can see that the attack method for such defacement has become more sophisticated. The other causes for website defacement include: **FTP account information** which is used for uploading contents files was **stolen**. There have been a number of such cases in 2012 (as in 2011). We assume that the PCs used for such upload were infected with a virus.

Even if you implement countermeasures on your website, it would not make sense if you allowed for the leakage of your FTP account information from your PC. Website administrators are encouraged to implement not only countermeasures for system administrators but also countermeasures for PCs for individual users.

Countermeasures for System Administrators

- **Perform strict control and settings of IDs and passwords**
- **Eliminate security holes (including operational workaround if no patch is applicable)**
- **Perform appropriate settings and access control of routers and firewalls**
- **Perform periodical log checking**

Countermeasures for Individual Users

- **Keep your antivirus software up-to-date**
- **Update your OS and applications (e.g., by applying Windows Update and Office Update)**
- **Perform appropriate password settings and control (make them complex, do not tell them to others, do not use the same password for multiple purposes etc.)**
- **Consider making use of routers and personal firewalls**
- **Check for your wireless LAN encryption settings (When possible, use WPA2 instead of WEP)**

As for the cases other than website defacement, what stood out were: services such as online games being logged in and used by someone else by means of spoofing, which caused monetary damage; and a port used for SSH being penetrated by an attacker (mainly caused by "Poor ID & password management" and "Unknown") and being used as a steppingstone for attacking other computers. Most of the cases were caused by "unknown" factors, but fundamental security measures do serve as effective countermeasures. So, please feel free to use the following information.

Information for System Administrators

- iCat – A Security Alert Service for Cyber Security
  http://www.ipa.go.jp/security/vuln/icat.html (in Japanese)
- "Educational Materials for Information Security"
  http://www.ipa.go.jp/security/fy18/reports/contents/ (in Japanese)
- "Checkpoint for Vulnerability Countermeasures"
  http://www.ipa.go.jp/security/vuln/20050623_websecurity.html (in Japanese)
- "How to Secure Your Website 6th. Edition"
  http://www.ipa.go.jp/security/vuln/websecurity.html (in Japanese)

・"JVN (Japan Vulnerability Notes)" *Vulnerability Information Portal Site
http://jvn.jp/ (in Japanese)

・"Security Alert on SQL Injection Attack"
http://www.ipa.go.jp/security/vuln/documents/2008/200805_SQLinjection.html (in Japanese)

・"Security Alert on Websites where Older Versions of Software Products are Used"
http://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html (in Japanese)

・"To Website Administrators: Security Alert on Website Defacement"
http://www.ipa.go.jp/security/topics/20091224.html (in Japanese)

・Registration for "IPA Mail News"
http://www.ipa.go.jp/about/mail/ (in Japanese)

Information for End Users/Home Users

・"Security can be Started from Here", Information Security Portal Site
http://www.ipa.go.jp/security/kokokara/ (in Japanese)

・" IT Security Center, IPA" - Web Pages for Individual Users"
http://www.ipa.go.jp/security/personal/ (in Japanese)

・"Microsoft Security Center" (Microsoft, Japan)
http://www.microsoft.com/ja-jp/security/default.aspx (in Japanese)

・MyJVN (Security Settings Checker, Version Checker)
http://jvndb.jvn.jp/apis/myjvn/ (in Japanese)

・A Spate of Unauthorized Accesses to Internet Banking Systems in the Nation
http://www.ipa.go.jp/security/topics/alert20110803.html (in Japanese)

(2) Damage Instance

[Intrusion]

(i) Our Website was defaced through the exploitation of CMS plug-in vulnerabilities

Instance	- We were informed by an external party: "your Website has been defaced." Upon checking it, we found that some pages had been altered. - The display screen image contained a religious picture and text. Upon checking what had been altered, we found that the alteration had been limited to the display contents, and fortunately, no collateral damage (e.g., virus infection) had been made to the site visitors. - Vulnerabilities within JCE*1, which is a plug-in for feature expansion of a CMS*2 called "Joomla!" was exploited and a backdoor was embedded into our server. Through the backdoor, the attacker broke into our server and performed such alteration. - After the incident, we stopped using "Joomla!" and instead, decided to directly change HTML when updating our website.

*1 JCE: Software for editing "Joomla!"-based web pages.
*2 CMS (Content Management System): Application software which enables users to manage their Website contents (text and pictures) in a comprehensive manner.

［DoS］

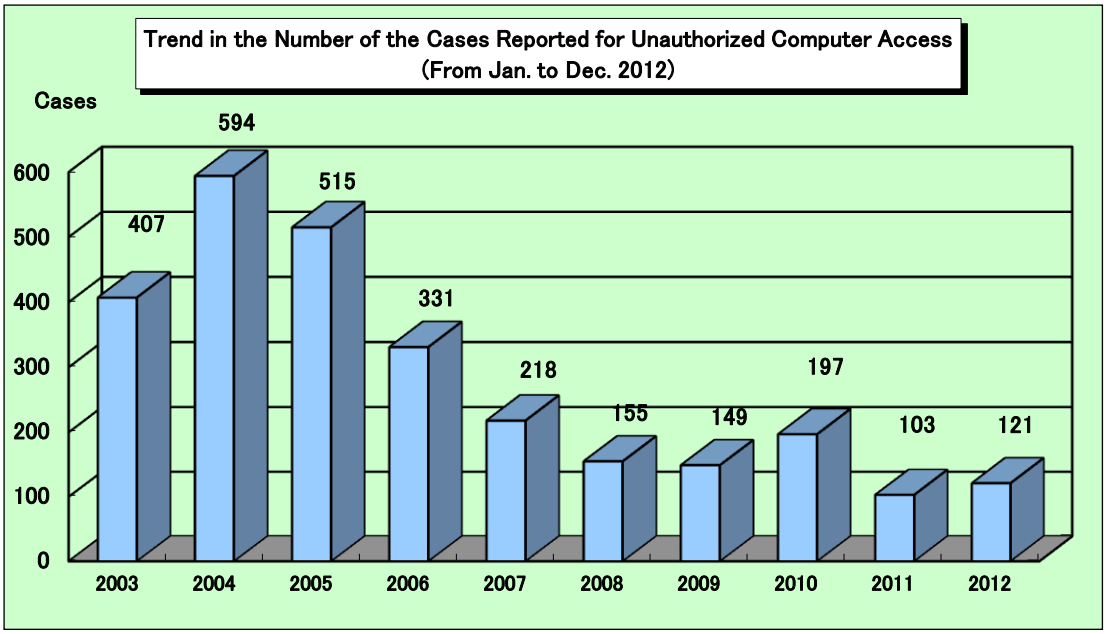
(ii) Our internet connection was paralyzed due to a large volume of accesses from multiple IP addresses

Instance	- I'm providing a game server*3 on the Internet through my home Internet connection. This allows unspecified number of people to play. One day, all of a sudden, I became unable to access the Internet. - Upon checking my home router's logs, I found that a large volume of packets had been sent to a certain IP address. I assume that my home Internet bandwidth was exhausted through Dos Attack. - I configured my firewall to reject any access from that IP address, but the following day, such access was made from another IP address, so there is no end to this trouble no matter how I thoroughly implement countermeasures. - I have no idea about effective countermeasures against this type of DoS attack. I'm in trouble.

*3 Providing a game server: Depending on the nature of the game, it might be prohibited to provide such game on the Internet. So, when you release any game, prior confirmation is required.

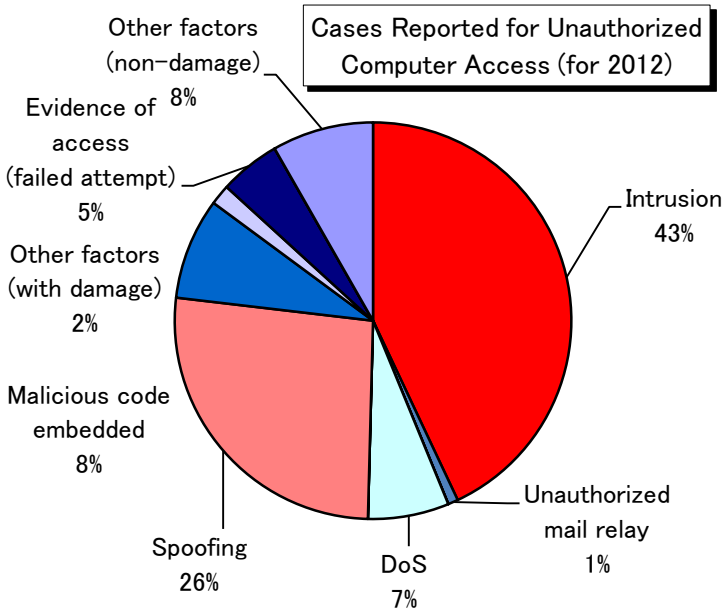
(3) Number of the Cases Reported

The number of the cases reported throughout the year 2012 was **121, up** 18 (or about 17 percent) from 103 in 2011. The graph below shows the past-ten-year trend in the number of the cases reported to IT Security Center, IPA.



(4) Type of Reports

Compared to 2011, the number of the cases reported for "Intrusion" and "Spoofing" increased in 2012, which contributed the increase in the total number of the cases involving actual damages.

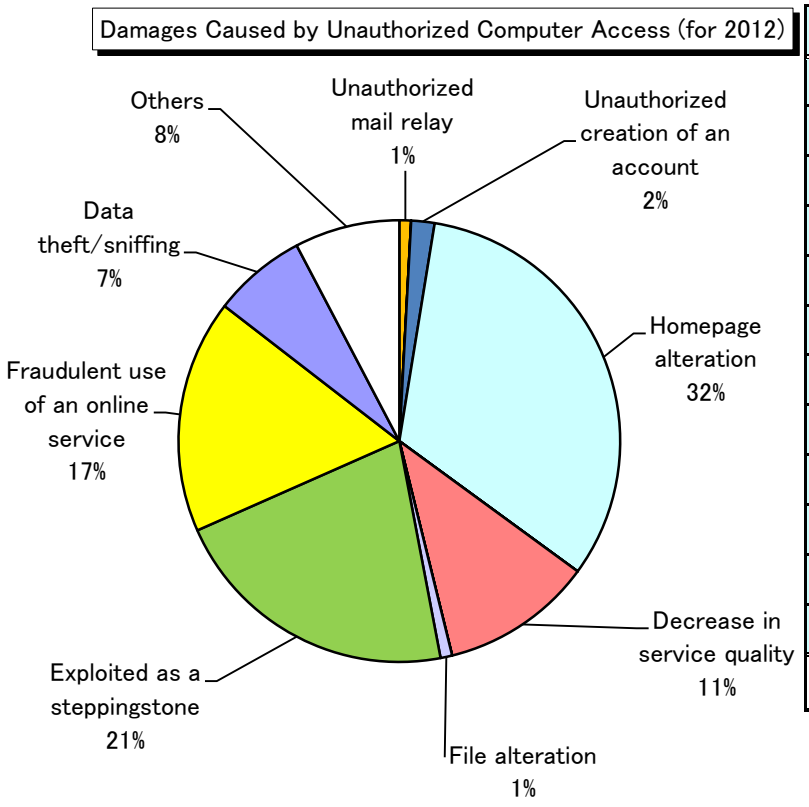


Type of Report	YR2012	YR2011
Intrusion	52	39
Unauthorized mail relay	1	1
Worm infection	0	0
DoS (Denial of Service)	8	5
Spoofed address	0	0
Spoofing	32	25
Malicious code embedded	10	5
Other factors (with damage)	2	0
Evidence of access (failed attempt)	6	21
Evidence of Worm	0	0
Other factors (non-damage)	10	7
Total	**121(105)**	**103(75)**

* Shaded regions as well as the figures in the parentheses indicate the cases involving actual damages.

(5) Damages Caused

Breakdown of the cases involving actual damages is shown below. The number of the cases involving actual damages has increased by 30 cases (or 40 percent) from the previous year level. In particular, the number of the cases reported for "**Website defacement**" has increased.

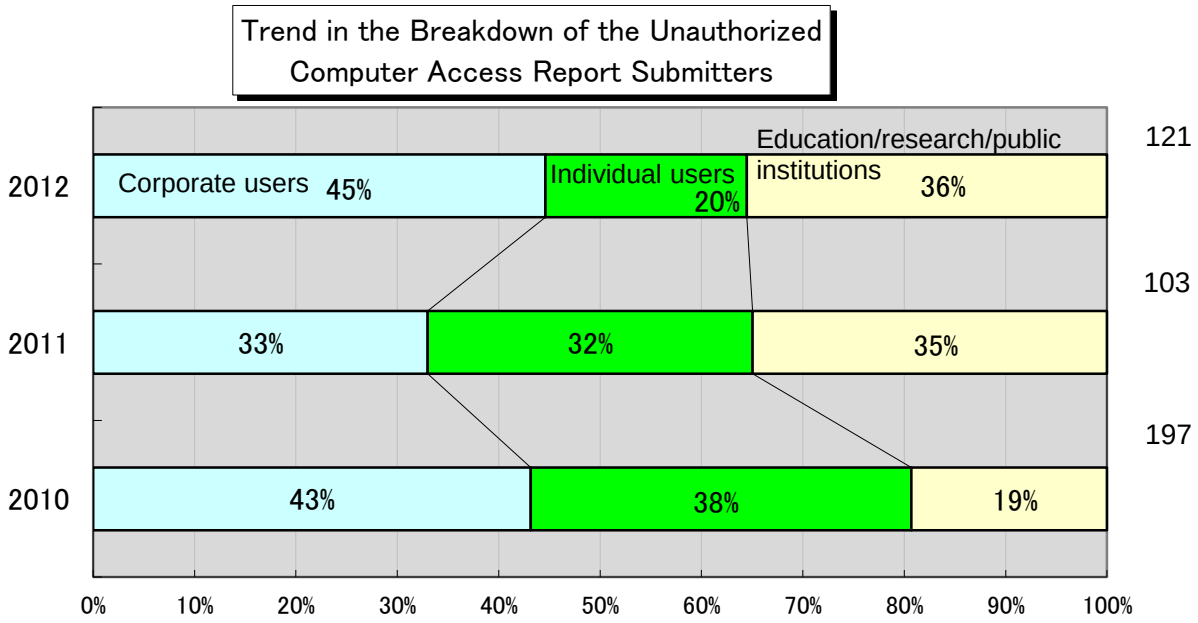


Damage	YR2012	YR2011
Unauthorized mail relay	1	1
Servers brought down	0	0
Unauthorized account creation	2	1
Website defacement	38	13
Theft and Use of password files	0	0
Service degradation	13	7
Open proxy	0	0
File alteration	1	4
Exploited as a steppingstone	25	27
Unauthorized use of online services	20	17
Theft of and spying on data	8	8
Others	9	3
Total Cases	**117(*)**	**81(*)**

* Since one actual damage report may contain multiple damages, the sum of the actual damage reports may not equal to the figures in the Total Cases column in the above table.

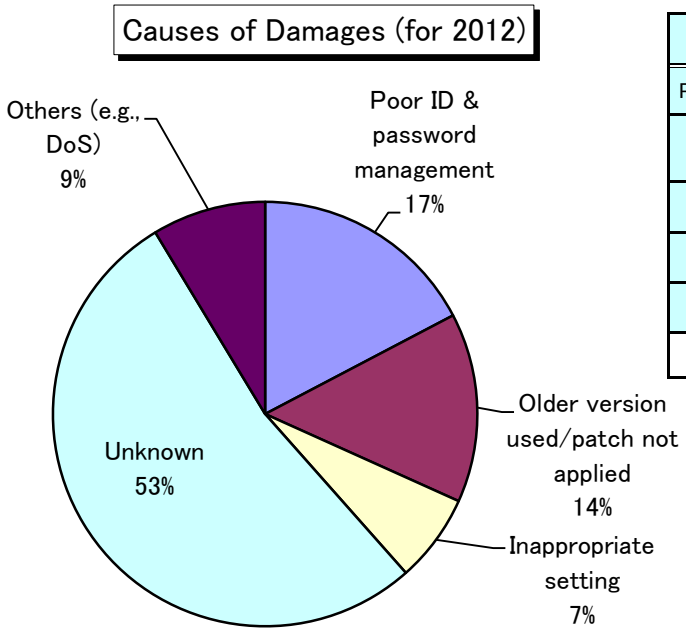
(6) Damages Caused

Breakdown of the report submitters is shown below. The number of the cases reported from "Corporate Users" has increased from the previous year level. This is due to the fact that the cases involving website defacement at general enterprises have increased.



(7) Causes of Damages

Breakdown of the cases involving actual damages in terms of causes is: "Poor ID & password management" (18 cases (17 percent)); "Older version used/patch not applied" (15 cases (14 percent)); "Inappropriate setting" (7 cases (7 percent)); and "Unknown" (56 cases (53 percent)). As in 2011, the cases in 2012 caused by "Unknown" factors accounted for almost half of the total, **so we can assume that unauthorized computer access cases that are difficult to probe the cause is on the increase.**



Cause of Damage	YR2012	YR2011
Poor ID & password management	18	15
Older version used/ patch not applied	15	12
Inappropriate setting	7	11
Unknown	56	32
Others (e.g., DoS)	9	5
Total Cases	**105**	**75**

Inquiries to:
Kagaya/Aoki at IT Security Center, Information-technology Promotion Agency, Japan
Tel:03-5978-7591
E-mail: isec-info@ipa.go.jp

3. Consultation

(1) General Overview for the Year 2012

The number of the cases consulted for computer virus and unauthorized computer access from January to December 2012 was **11,950**, **2,755** of which were related to **"One-click Billing Fraud"**; **354** to **"Fake Security Software"**; **125** to **"Winny"**; **40** to **"A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data"**.

The year 2012 trend in the total number of the cases consulted for computer virus and unauthorized computer access is shown in Figure 3-1 and Table 3-1. The number of the cases consulted decreased temporally in March and April. As mentioned in the "General Overview for the Third Quarter of 2012", this is due to the influence of the arrest for "**One-click Billing Fraud**", which took place in December 2011. The number of the cases consulted increased temporally in October. This is due to the influence of "**Remote Operation Virus**", which grabbed headlines in the last year. Depending on the reported month, we saw a slight up-and-down trend, but generally, the number remained roughly flat.

We also tallied the number of the cases consulted for "One-click Billing Fraud", "Fake Security Software", "Winny", and "Suspicious E-mails". As for "One-click Billing Fraud" and "Winny", the number remained roughly flat, and as for "Fake Security Software", the number showed an increasing trend.

In addition, when we saw the trend in the number of the cases consulted that contained the keyword "smartphone", as shown in the "General Overview for the Third Quarter of 2012", the number is still small, but it is obviously showing an increasing trend, so we expect it to increase further in the future.

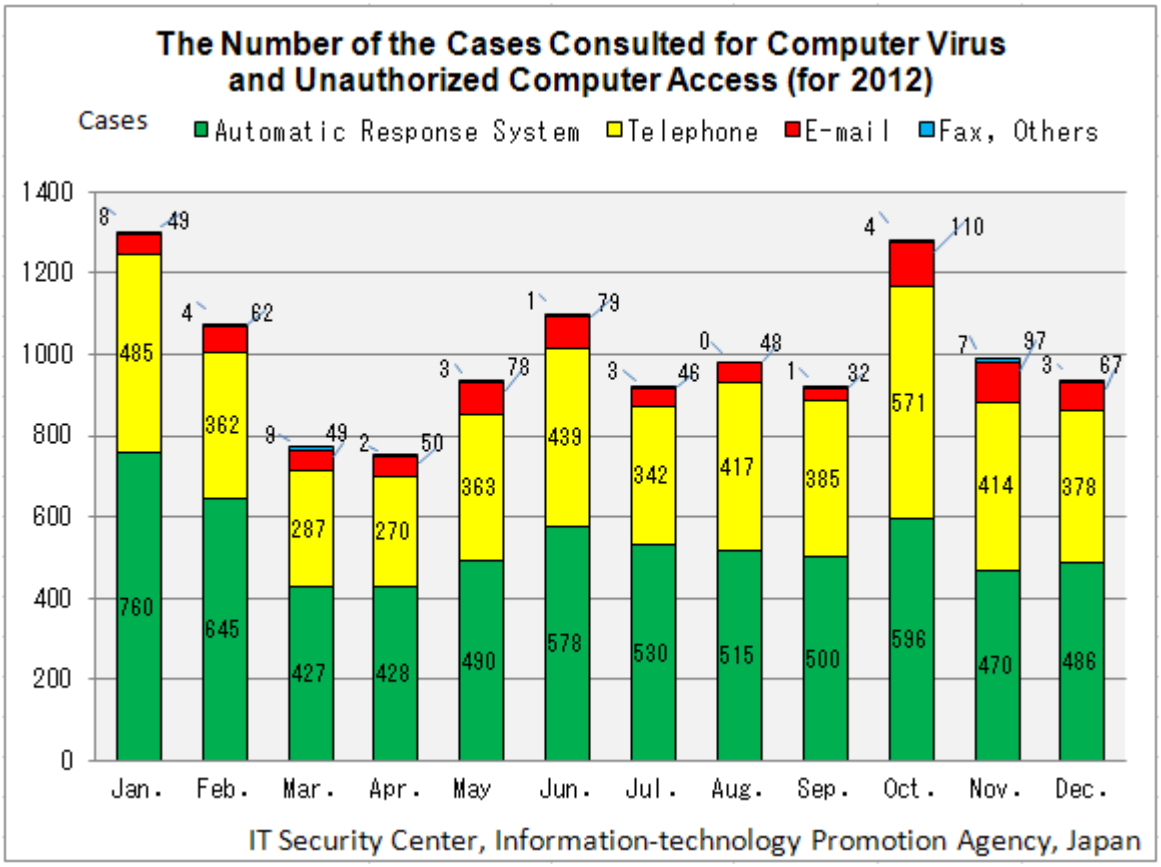


Figure 3-1 : Trend in the Number of the Cases Consulted for Computer Viruses and Unauthorized Computer Access (in Total for 2012)

Table 3-1: the Number of the Cases Consulted for Computer Viruses and Unauthorized Computer Access

	YR2012											
	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.	Aug.	Sep.	Oct.	Nov.	Dec.
Total	11,950											
	1,302	1,073	772	750	934	1,097	921	980	918	1,281	988	934
Automatic Response System	760	645	427	428	490	578	530	515	500	596	470	486
Telephone	485	362	287	270	363	439	342	417	385	571	414	378
E-mail	49	62	49	50	78	79	46	48	32	110	97	67
Fax, Others	8	4	9	2	3	1	3	0	1	4	7	3

(2) Consultation Instances

Major consultation instances are as follows:

(i) I accidentally downloaded suspicious software and since then, I became unable to access the Internet

What was consulted	When I visited a Website, a pop-up window appeared. I tried to close it and clicked it, but without my knowing, suspicious software was downloaded and installed. When I tried to access the Internet, a warning message "You are trying to access a suspicious Website" is issued by this software and I was unable to access the Internet. Could you tell me how I can address this problem?
Response	We assume that your PC has been infected with so called "fake security software". This sort of software claims to "speed up your PC" or "detect viruses" so that it looks like useful software but in fact, it is designed to issue a bogus warning message and urge PC users to buy certain paid software. So even if you see such pop-up window, do not enter your credit card number or other personal information. Should you enter your credit card number or other personal information, consult your credit-card company and the consumer affairs bureau and consider changing your card number. As for the infected PC, it is recommended to perform "system restoration", which enables it to restore the state before the infection. If you are unable to solve the problem, you need to perform "initialization" on that PC. Furthermore, in order to prevent such damages in the future, keep up-to-date your operating system, application software, and antivirus software. <Reference> "Never-Ending Cases Involving Viruses that Issue a Bogus Warning Message" http://www.ipa.go.jp/security/txt/2012/03outline.html#5 (in Japanese)

(ii) When I was using Internet banking, a suspicious window appeared and I entered my authentication number

What was consulted	When I logged in, a pop-up window appeared and I was prompted to enter my login password and test word. So I entered them. Later I learned from the news etc. that there had been a number of incidents where a bogus login screen for Internet banking was used for fraud. How can I cope with it?

Response	In the case of a login from environments other than normal one, a window may appear in which you are asked to enter your login password and test word (i.e., risk-based authentication). But while you were using Internet banking, a suspicious pop-up window appeared and you entered your login password and test word, right? Firstly, contact immediately the "person to contact" of your Internet banking for authenticity and if confirmed to be a bogus entry screen, ask the person how you can prevent your money from being withdrawn from your bank account. After that, update your antivirus software to the latest and perform a virus scan on your PC. It is recommended to perform a multilateral scan by using online scan services provided by other companies. If you find a virus, you may be able to clean it with that antivirus software. But just in case, it is also recommended to perform "system restoration" or "initialization" on your PC and then to log in from the legitimate login screen and change your password and test word. Furthermore, in order to prevent such damages in the future, keep up-to-date your operating system, application software, and antivirus software. <Reference> "Watch Out for a Malicious Pop-up Window that Exploits Net Banking" http://www.ipa.go.jp/security/txt/2012/12outline.html#5 (in Japanese)

（3） Detail Analysis of the Cases Consulted

Table 3-2 shows our comparison result of the number of the cases consulted throughout the Year 2011 and the Year 2012. As shown in this table, compared to the number of the cases consulted throughout the Year 2011, the number for the Year 2012 decreased. This is due to the fact that IPA provided FAQs regarding "One-click Billing Fraud", which account for an important share of the total cases consulted (as analyzed in the "General Overview for the Third Quarter of 2012"), and it is clear from the estimated website traffic for the year 2012 to IPA's security alert pages concerning "One-click Billing Fraud" (approximately 189,000 accesses per year, which is approximately 15,750 accesses per month).

As for the number of the cases consulted for fake security software, we have seen it increase and decrease every few years; in fact, between 2010 and the first half of 2011, the number of the cases consulted decreased, but between the second half of 2011 and 2012, the number increased. This indicates that new types of fake security software began to emerge in the market (see Figure 3-3). Meanwhile, one of the special instructions for the year 2012 concerning fake security software is: **"increasingly atrocious nature" of fake security software**. In fact, such fake security software existed previously and a large number of such cases have been reported so far. However, the fake security software that appeared at the end of last year has characteristics of "making the infected PCs unable to access the Internet" and "intercepting an attempt to restore the infected systems" etc. So **once infected, the PC has no choice but to perform initialization**. So far, IPA has received inquiries concerning this fake security software.

Table 3-2: A Comparative Table for the Number of the Cases Consulted (2011 versus 2012)

Year and the Number of Cases (NoC)		NoC Consulted (in Total)	One-click Billing Fraud	Fake Security Software	Winny	Suspicious E-mail	Smartphone
YR 2012	NoC	11, 950	2, 755	354	125	40	273
YR 2011	NoC	18, 567	5, 509	96	151	38	126
Increased/Decreased by	NoC	−6, 617	−2, 754	258	−26	2	147
Increased/Decreased by	Percent (%)	−36%	−50%	269%	−17%	5%	117%

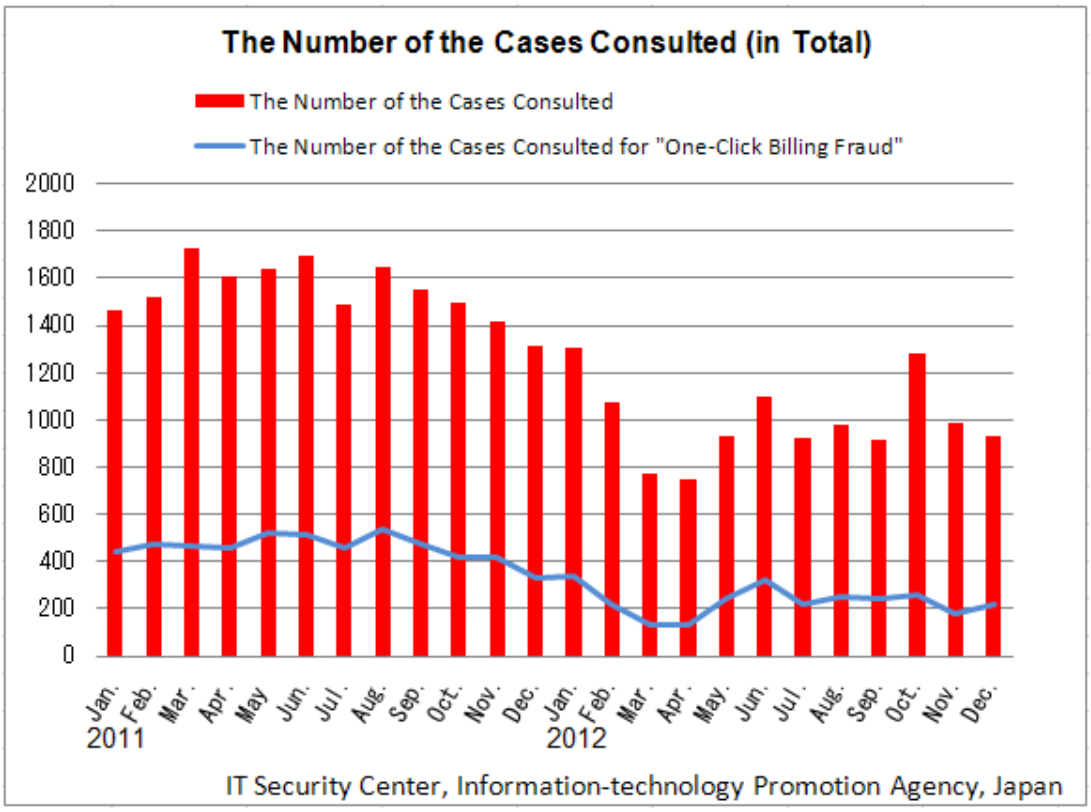


Figure 3-2：Trend in the Number of the Cases Consulted (Between 2011 and 2012)

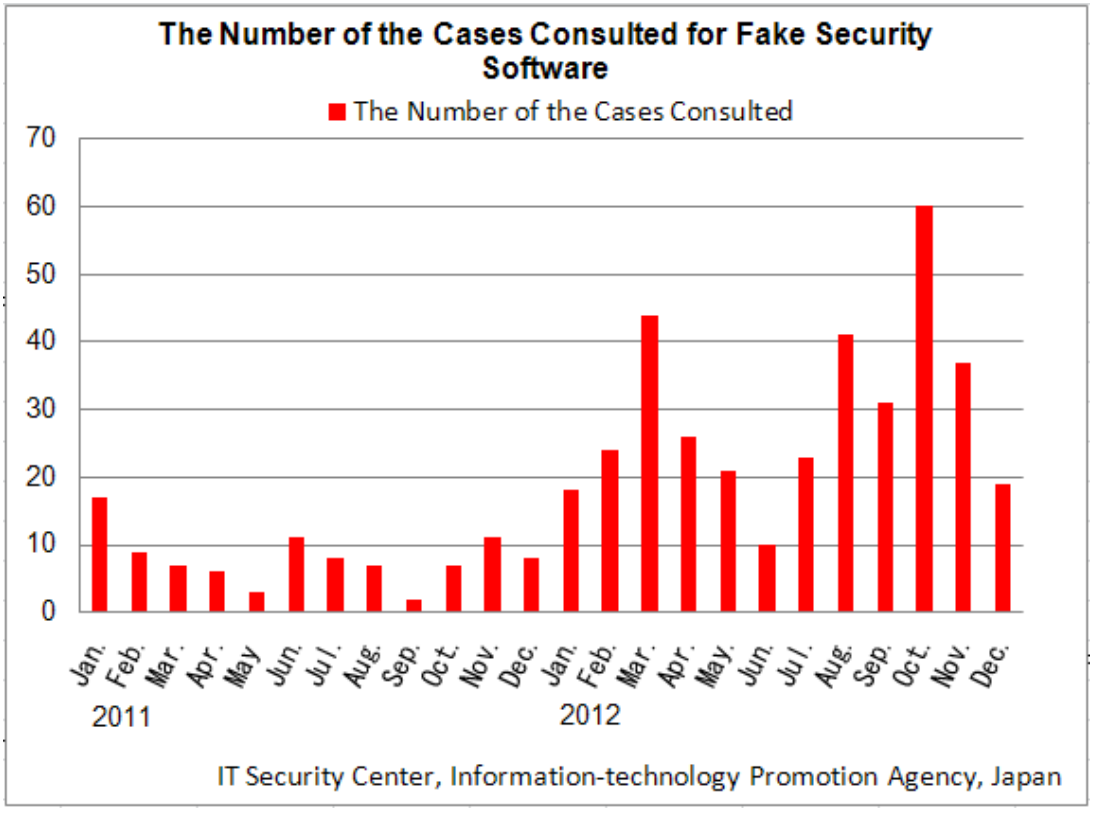


Figure 3-3：Trend in the Number of the Cases Consulted for Fake Security Software

Figure 3-4 shows the results of our tallying for the cases consulted for smartphone (NB: we performed a keyword search), which is worth noticing for the future. From this result, we can see that along with the popularization of smartphone in recent years, the number of cases consulted has also been increasing. The number is expected to increase further in the future.

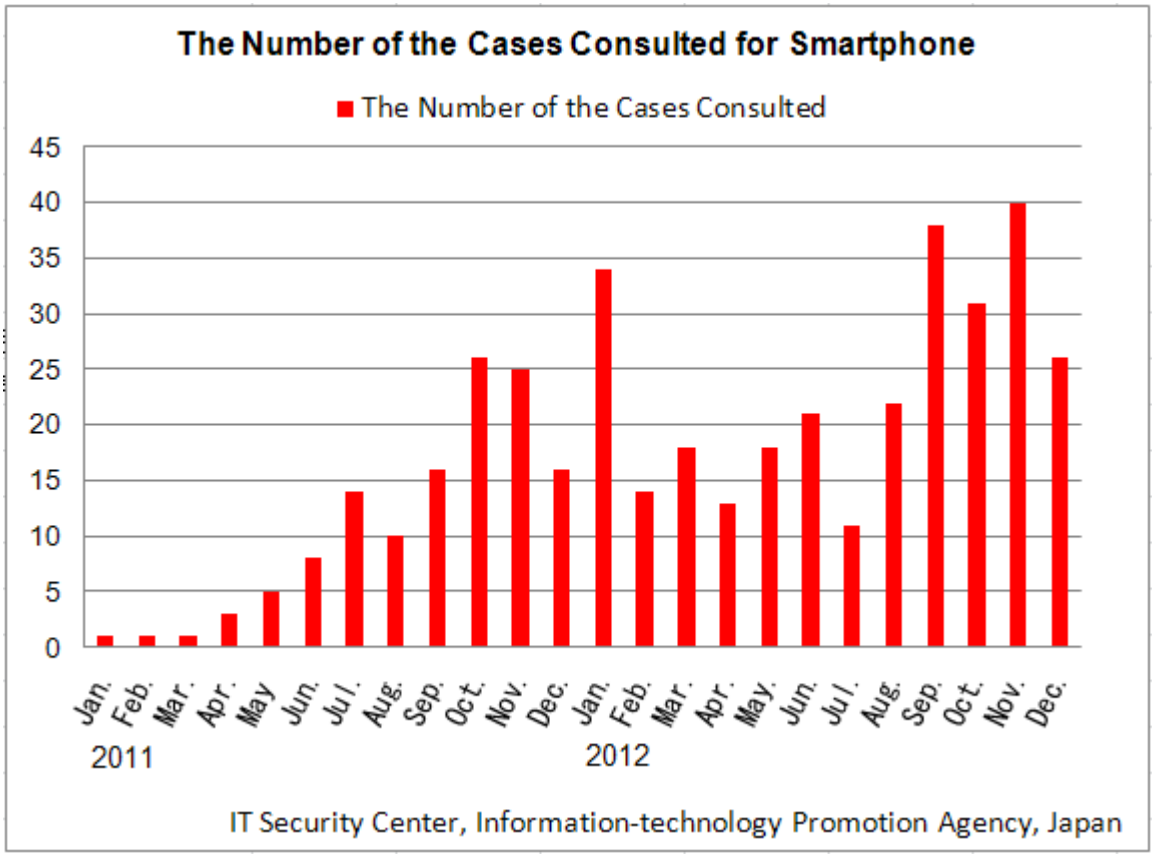


Figure 3-4 : Trend in the Number of the Cases Consulted for Smartphone

Inquiries to:
Kagaya/Aoki at IT Security Center,
Information-technology Promotion Agency, Japan
Tel:03-5978-7591
E-mail: isec-info@ipa.go.jp