Computer Virus/Unauthorized Computer Access Incident Report - September 2011 -

This is the summary of computer virus/unauthorized computer access incident report for September 2011, compiled by Information-technology Promotion Agency, Japan (IPA).

I. Reminder for this Month

"Watch out for new type of phishing scam that uses a virus!"

The last month's reminder was about unauthorized use of Internet banking by the SpeEye virus. While the SpeEye steals information entered on a keyboard, IPA confirmed in September 2011 another case in which a different technique was used to steal login information for Internet banking.

The technique involved the combination of an existing phishing technique and a virus. Specifically, an e-mail which is spoofed as the one from a bank is sent to the target along with a virus in the form of attachment; if the virus is executed, a screen appears, prompting the e-mail recipient for login information and/or to fill in a random table; if the e-mail recipient enters such information as instructed, the information falls into the hands of a malicious entity. In fact, there has been a case in which a total of millions of yen has been withdrawn from a bank account by this means.

IPA obtained a fake e-mail that has actually been used and analyzed the virus attached to it. Remainder of this section presents an outline of the virus and how it works when executed as well as how to avoid suffering from it, all of which was derived from the analysis results.

(1) What is Phishing?

Phishing is an act of sending an e-mail which is spoofed as the one from a financial institution (bank, credit card company) or other organizations, getting the e-mail recipient to access a fake website, and fraudulently obtaining his/her personal information such as home address, name, bank account number and credit card number.

A typical phishing case is described below (see Figure 1-1).

![Figure 1-1: Flow of a Typical Phishing Case](image)

[I] The attacker sends a fake e-mail

The attacker indiscriminately sends an e-mail which is spoofed as the one from a legitimate web service, a financial institution or other existing organizations.

[II] The PC user clicks a link in the e-mail message

Trusting that e-mail, the recipient clicks a link (URL) in the message, for which he is guided to a
fake website prepared by the attacker in advance.

[III] The attacker obtains the login information entered
Without noticing that this is a fake website, the PC user enters login information (such as ID and password), for which the account information falls into the hands of the attacker.

[IV] The attacker logs into the authentic website
Using the login information obtained, the attacker logs into the authentic website, spoofing as the PC user.

(2) Outline of New Type of Phishing Technique that Uses a Virus
This section explains the virus behavior and techniques applied that have been confirmed by IPA.

[I] An e-mail that serves as a trigger
The e-mail message looks like the one from a big bank in the nation and a virus is attached to the e-mail (see Figure 1-2).

Upon investigating the attached file, we found that this was a type of a virus called "Banker" or "Jginko". Its icon resembles an existing bank's logo and apparently, it is aimed at having the recipient click it without question (see Figure 1-3).
[II] Login information entry screen
If the e-mail recipient opens the attached file as instructed in the message, a screen appears, prompting him/her for contract number and password and/or to fill in a random table, as you would be asked when you remit money (See Figure 1-4). Generally, such request is not made by e-mail.

[III] Transfers the login information entered
If the e-mail recipient enters information and clicks the "Send" button, the entered information is transferred to an external server in the form of screen image. If an attempt to connect to the external server fails, a garbled message is displayed. In
Japanese environment, the garbled character string should resemble the one shown in the figure below, which is expressed as 连接失败 in simplified Chinese and translated as “connect failure”. Hence this virus could have been created by someone who understands Chinese.

![Figure 1-5: A Message that Appears When a Connection Failure Occurs](image)

[IV] **A malicious entity can log in**

Since the Internet banking user’s contract number, multiple passwords and all the information in the random table fall in the hands of the malicious entity, he might used them to log in to the Internet banking site and perform operations such as remitting money.

(3) **Countermeasures**

In the traditional phishing technique, a malicious entity had to establish a fake website and to guide PC users to the fake site, but in the case of the phishing technique confirmed this time, an e-mail attachment itself contains a mechanism to have its recipients enter their account information, so its mechanism is simple.

The simpler the mechanism, the more important it is to ensure that basic countermeasures are implemented.

[I] **Countermeasures against phishing**

(1) **Check for the authenticity of that e-mail**

Even if the e-mail you received seems to be from an existing financial institution, check carefully for the message. First, **such a request (i.e., asking for your card number or PIN) should never be made by e-mail.** If you received such e-mail from a financial institution or other organizations, call the e-mail sender or refer to the notification column in their website to check for the authenticity of that information (e-mail). When you make a telephone inquiry, do not call the number written in the e-mail message; instead, check first for the correct contact number (e.g., by referring to the document that was sent to you at the time of opening of your account) and then make a call.

(2) **Watch out for a link in the e-mail message**

It is also important not to click a link in an e-mail message carelessly. When you check the website of the bank in question, refrain from accessing it by clicking a link in the e-mail message. It is recommended to register its correct address in your browser’s “favorite website” or “bookmark” so that you can always access it from there.

<Reference>
Council for Countermeasures for Phishing

[II] **Countermeasures against the virus**
(1) **Handling of E-mail attachments**

   If any file is attached to the e-mail you received, always suspect that it could be a virus. Even if the e-mail is from someone you know well, you should exercise caution. If you feel suspicious about the e-mail, contact its sender for confirmation or delete it without opening it.

(2) **Make use of antivirus software**

   By installing antivirus software and keeping its virus list up-to-date, you can prevent the invasion of viruses and clean any viruses already entered. If antivirus software has already been installed, the virus that is used in the aforementioned case could also be detected as it checks for viruses when the PC receives an e-mail, saves an attached file, or opens a file.

[III] **Post-incident response**

   Should you suffer from unauthorized use of your Internet banking service, contact the processing bank. Most banks provide a means for their users to send inquiries from the front page of their website. In addition, by using a non-infected, safe PC that is under your control, change your password for the Internet banking service. If you fall for "Banker" or "Ginko", which is a type of phishing scam that prompts the victim to fill in a random table, the data in the table falls in the hands of the malicious entity. So you need to change your random table card, or reopen your account.

   Remember that ID and password management is one of the essential countermeasures; for more details, refer to the reminder of the June 2011 issue.

<Reference>

Reminder of the June 2011 issue, "My password is a treasure unknown to anybody other than myself" (IPA)

II. Computer Virus Reported – for more details, please refer to Attachment 1 –

(1) Computer Virus Reported

While the virus detection count \(^1\) in September was about 21,291, down 15.3 percent from about 25,143 in August, the virus report count \(^2\) in September was 906, down 2.7 percent from the August level (931).

\(^1\) Virus detection count: indicates how many times a specific virus appeared in the reports submitted, or the aggregate virus detection counts for a specific period.

\(^2\) Virus report count: indicates how many reports on a specific virus were submitted. If the same type of viruses were reported by the same person with the same detection day, they are counted as one report regarding the virus of that sort.

\(^*\) In September, the virus report count, which was obtained by consolidating about 21,291 virus detection reports, was 906.

*W32/Mydoom* marked the highest detection count at about 9,525, followed by *W32/Netsky* at about 9,194 and *W32/Autorun* at about 553.

\[\text{Figure 2-1: Virus Detection Count}\]

\[\text{Figure 2-2: Virus Report Count}\]
(2) Malicious Programs Detected

In September, DOWNLOADER which refers to a malicious program that attempts to infect the victim's PC with another virus was on the increase. Meanwhile, a malicious program called RLTRAP has increased significantly in September (See Figure 2-3). RLTRAP is a general term for a malicious program whose file name extension is manipulated so that PC users take it for an ordinary file.

![Figure 2-3: Malicious Program Detection Count](image-url)
III. Unauthorized Computer Access Reported (including Consultations) – for more detail, please refer to Attachment 2 –

| Table 3-1: Unauthorized Computer Access Reported (including Consultations) |
|---|---|---|---|---|---|---|
| Total for Reported (a) | 5 | 7 | 9 | 8 | 10 | 7 |
| Damaged (b) | 5 | 6 | 9 | 5 | 8 | 5 |
| Not Damaged (c) | 0 | 1 | 0 | 3 | 2 | 2 |
| Total for Consultation (d) | 38 | 55 | 32 | 47 | 37 | 31 |
| Damaged (e) | 10 | 14 | 15 | 13 | 8 |
| Not Damaged (f) | 28 | 41 | 25 | 32 | 24 | 23 |
| Grand Total (a + d) | 43 | 62 | 41 | 55 | 47 | 38 |
| Damaged (b + e) | 15 | 20 | 16 | 20 | 21 | 13 |
| Not Damaged (c + f) | 28 | 42 | 25 | 35 | 26 | 25 |

(1) Unauthorized Computer Access Reported
The report count for unauthorized computer access in September was 7, 5 of which reportedly had certain damages.

(2) Unauthorized Computer Access and Other Related Problems Consulted
The consultation count for unauthorized computer access and other related problems was 31. 8 of them reportedly had certain damages.

(3) Damages Caused
The breakdown of the damage reports were: intrusion (2); Spoofing (3).
Damages caused by "intrusion" were: a web page being defaced (1); login information etc. was stolen from a database (1). Causes of "intrusion" were: a vulnerability in a web application being exploited (1); (other cases remain unknown).
Damages caused by "spoofing" were: an online service being used by someone who successfully impersonated a legitimate user and logged on (3 cases for online games).

(4) Damage Instance

[i] Login information and other information were stolen by SQL injection attack

<table>
<thead>
<tr>
<th>Instance</th>
<th>- Since the response of our published website became abnormally slow, I inspected it and found the trace of an unauthorized access.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- After analyzing the access log in detail, the unauthorized access was found to have been caused by SQL injection attack.</td>
</tr>
<tr>
<td></td>
<td>- As for the section that received the attack this time, vulnerability to such attack had been remedied two years before, but the section became vulnerable again due to the source degradation* that occurred at the time of updating web pages and as a result, was exploited for the attack.</td>
</tr>
</tbody>
</table>

*Degradation: when modifying a part of a program, other parts might be set back to a previous vulnerable state. This is called degradation.
[Spoofing]

(ii) My account for an online game was taken over

<table>
<thead>
<tr>
<th>Instance</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>While I was playing a game, I was told by a participant that &quot;I'll give you some in-game money&quot;, so I told him my password. Then at a later date, I became unable to log into the game.</td>
</tr>
<tr>
<td></td>
<td>Apparently, he changed my password after a successful login with my account.</td>
</tr>
<tr>
<td></td>
<td>Do the police accept an offense report on spoofing like this?</td>
</tr>
</tbody>
</table>
IV. Virus and Unauthorized Computer Access related Consultations

The total number of consultations in September was 1,551. 477 of which were related to "One-Click Billing" (compared to 535 in August); 2 to "Fake Security Software" (compared to 7 in August); 19 to "Winny" (compared to 7 in August); 2 to "A Suspicious E-Mail Sent to a Specific Organization to Collect Specific Information/Data" (compared to 0 in August).

Table 4-1: Total Number of Consultations Handled by IPA over the Past Six Months

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1,608</td>
<td>1,640</td>
<td>1,692</td>
<td>1,490</td>
<td>1,651</td>
<td>1,551</td>
</tr>
<tr>
<td>Automatic System</td>
<td>997</td>
<td>950</td>
<td>999</td>
<td>889</td>
<td>958</td>
<td>936</td>
</tr>
<tr>
<td>Telephone</td>
<td>555</td>
<td>620</td>
<td>639</td>
<td>540</td>
<td>639</td>
<td>554</td>
</tr>
<tr>
<td>e-mail</td>
<td>50</td>
<td>62</td>
<td>50</td>
<td>54</td>
<td>50</td>
<td>52</td>
</tr>
<tr>
<td>Fax, Others</td>
<td>6</td>
<td>8</td>
<td>4</td>
<td>7</td>
<td>4</td>
<td>9</td>
</tr>
</tbody>
</table>

* IPA set up "Worry-Free Information Security Consultation Service* that provides consultation/advises for computer virus, unauthorized computer access, problems related to Winny as well as overall information security.

E-mail address: anshin@ipa.go.jp
Tel.: +81-3-5978-7509 (24-Hour Automatic Response; Consultations are provided by IPA Security Center personnel and 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
*Total Number includes the number in the Consultation (d) column in the Table 3-1, "III. Unauthorized Computer Access Reported (including Consultations)."

![Number of the "One-Click Billing" Cases Consulted](chart.png)

Figure 4-1: Number of the "One-Click Billing" Cases Consulted
Major consultation instances are as follows:

(i) **Suffered from unauthorized access to a Rakuten service in use**

<table>
<thead>
<tr>
<th>What was consulted</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>I'm using a service provided by Rakuten. One day, I found the trace of a credit-card transaction which I do not remember. Apparently, somebody cracked my login password and used it to access the service (to make the purchase). In the case like this, what kind of actions should I take? (Three more similar cases were reported)</td>
<td>First, report this case to Rakuten immediately. Contact information for each service is posed in Rakuten's website below. To avoid suffering from similar incidents in the future, it is recommended to review your password security countermeasures. &lt;Reference&gt; Countermeasures against unauthorized use of Rakuten services [contact information is attached to the end of the page] <a href="http://corp.rakuten.co.jp/security/knowledge/answer.html">http://corp.rakuten.co.jp/security/knowledge/answer.html</a> (in Japanese) &lt;Reference&gt; Reminder of the May 2010 issue, “My password is a treasure unknown to anybody other than myself” (IPA) <a href="http://www.ipa.go.jp/security/english/virus/press/201105/E_PR201105.html">http://www.ipa.go.jp/security/english/virus/press/201105/E_PR201105.html</a></td>
</tr>
</tbody>
</table>

(ii) **Worrying about the possibility of information leakage through a file sharing software that I once have installed**

<table>
<thead>
<tr>
<th>What was consulted</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once I've installed a file sharing software as I wanted to try it. However, I failed to make proper settings and did not use it in the end. Now I'm worrying about the possibility of information leakage from my PC. Another concern is, whether the file sharing software still resides in my PC. Is there any way to confirm them?</td>
<td>The fact that you stopped short of using that file sharing software means that the software was not connected to the network, so you don't need to worry about information leakage. By using &quot;Information Leakage Countermeasure Tool&quot; provided by IPA, you can check whether the file sharing software remains in your PC. If you want to use this tool, make an application in the web page below.</td>
</tr>
</tbody>
</table>
V. Access Status Captured by the Internet Fixed-Point Monitoring System (TALOT2) in September

According to the Internet Fixed-Point Monitoring System (TALOT2), 108,576 unwanted (one-sided) accesses were observed at ten monitoring points in September 2011 and the total number of sources was 45,285. This means on average, 361 accesses form 150 sources were observed at one monitoring point per day. (See Figure 5-1)

'Total number of sources*: Indicates how many sources in total were observed by TALOT2. If multiple accesses from the same source were observed at the same monitoring point/port on the same day, they are considered one access from the specific source on that day.

Since the environment of each monitoring point for TALOT2 is equivalent to that of general Internet connection, an equal number of such accesses are thought to be made in the Internet users’ system environment.

Figure 5-1: Daily, Averaged Number of Unwanted (One-Sided) Accesses and Sources at the Same Monitoring Point/Port per Month (April 2011 to September 2011)

The Figure 5-1 shows daily, averaged number of unwanted (one-sided) accesses and sources at the same monitoring point/port per month (from April 2011 to September 2011). As shown in this figure, the number of unwanted (one-sided) accesses in September has slightly increased, compared to the August level.

The Figure 5-2 shows the September-over-August comparison results for the number of unwanted (one-sided) accesses, classified by destination (port type). As shown in this figure, access to 3389/tcp, whose increase in late August was reported in the September 2011 issue, decreased temporally but began to increase again (See Figure 5-3).

3389/tcp is mainly used by RDP*1 and because a virus called Morto*2 was confirmed in August 2011 that exploits this port to spread its infection to Windows computers, accesses to this port may have been made as part of the virus infection activities.

IPA has not received any virus reports concerning “Morto”, but for Windows users who are using features like remote desktop, it is recommended to review their virus countermeasures and to take steps to prevent the virus infection, including strengthening their login passwords.

*1 RDP (Remote Desktop Protocol): A protocol that is used for remote desktop feature which allows Windows computers to be controlled remotely.

*2 Morto: A virus that infects Windows computers by exploiting RDP. After the infection, it performs port scan on
3389/tcp to search for computers whose remote desktop feature is activated, and then attempts password cracking against them.

**Figure 5-2: September-over-August Comparison for the Number of Accesses by Destination (Port Type)**

![September-over-August Comparison for the Number of Accesses by Destination (Port Type)](image)

**Figure 5-3: Access to 3389/tcp (Total Number of Accesses Observed at Ten Monitoring Points)**

![Access to 3389/tcp (Total Number of Accesses Observed at Ten Monitoring Points)](image)

For more detailed information, please also refer to the following URLs:
Attachment 3: Observations by the Internet Fixed-Point Monitoring System (TALOT2)
Variety of statistical Information provided by the other organizations/vendors is available at the following sites:

JPCERT/Coordination Center (CC) : [http://www.jpcert.or.jp/english/](http://www.jpcert.or.jp/english/)
@police : [http://www.cyberpolice.go.jp/english/](http://www.cyberpolice.go.jp/english/)

**Inquiries to:**
IT Security Center, Information-technology Promotion Agency, Japan (IPA/ISEC)
Kagaya/Miyamoto
Tel.: +81-3-5978-7591
Fax: +81-3-5978-7518
E-mail: isec-info@ipa.go.jp