Countermeasures against Targeted Attack Mail <Avoidance of Risks>

An attack that takes a shot at
a specific company/organization,
beginning with sending an e-mail!!

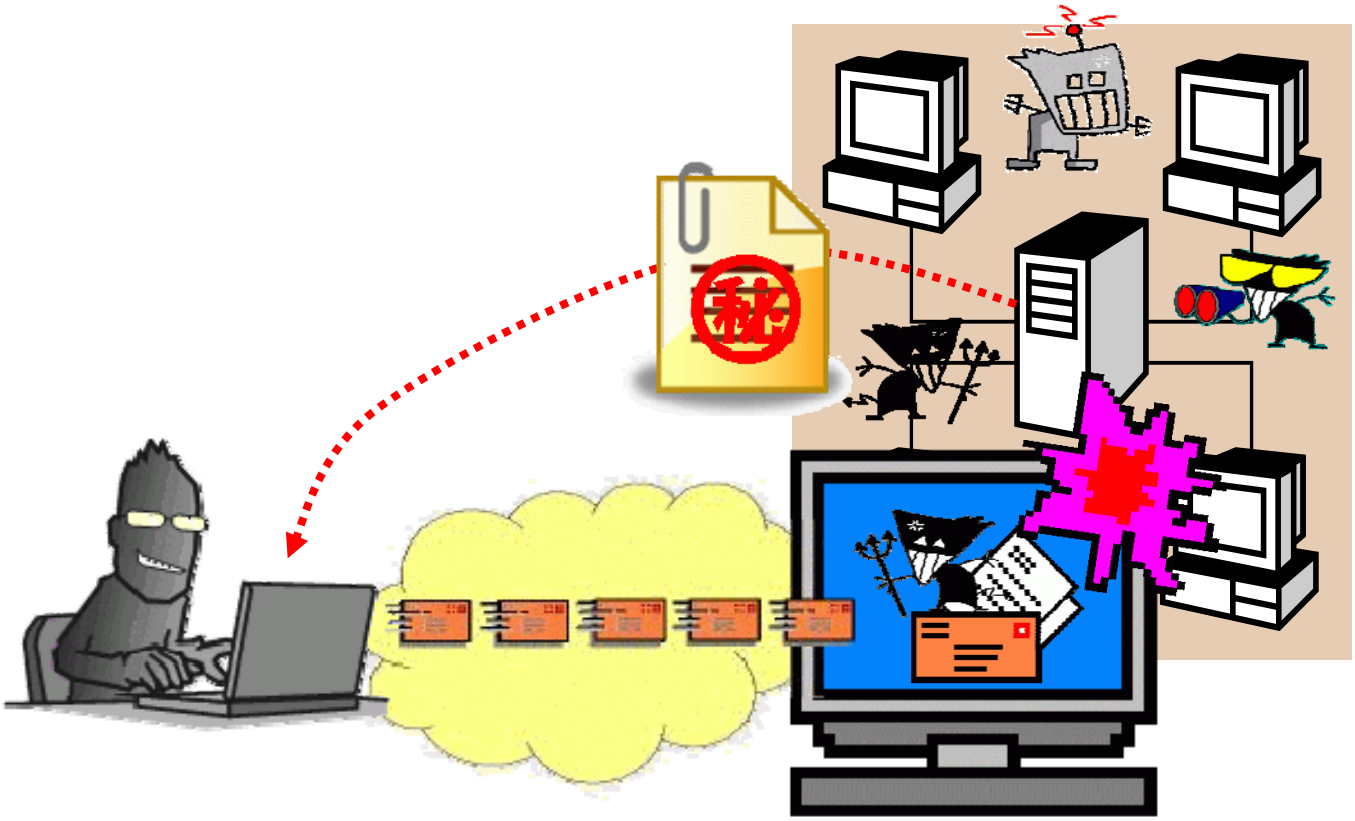
Information-technology Promotion Agency, Japan
IT Security Center

IPA 独立行政法人情報処理推進機構
セキュリティセンター

http://www.ipa.go.jp/security/ (in Japanese)

January 30, 2012 First Edition

Table of Contents



Introduction

This guide is written for company/organization employees and not for general computer users. We hope that this guide will be used for security education etc. within a company/organization.

"Targeted Attack" – an attack that takes a shot at a specific company/organization – is prevalent. In many cases, an e-mail posing as a government agency, a business associate, or a friend/acquaintance and carrying a computer virus is sent to the target as the onset of the attack.

To get the recipients to open its attachment, which would result in the execution of the virus contained*[1], a variety of "fraudulent techniques" are used to reduce their sense of distrust.

- A subject/main body doctored to attract the recipients' interest
- A sender posing as a person concerned
- An application file whose file name and icon are falsified so that it looks like a document file
- A document file that exploits vulnerabilities in operating systems or applications and executes an embedded code.

A variety of "fraudulent techniques" like these are used in combination to infect the recipients' PC with a virus.

Aren't you thinking that you will never be targeted or your company will not become the target of an attack?

Attackers are searching for sitting ducks and if they found one, they take a shot at it. Having security awareness in your day-to-day operation and implementing organized measures would protect yourself and your company against the clutch of such attack.

To avoid becoming a vulnerability (security hole) for your company/organization, implement day-to-day measures. If your PC is infected with a virus, security threats by the virus could spread throughout the company/organization. To avoid proving such breakthrough, follow appropriate security measure steps that comply with the security policy established by your company/organization.

*1) There is also an e-mail whose main body contains a link to a malicious website (i.e., the one that infects visitors' PC with a virus). Though such e-mail is not covered by this guide, watch out!

1. Targeted Attack and Targeted Attack Mail

"Targeted Attack" attacks a specific organization/individual, resorting primarily to an e-mail. A typical example confirmed is: sending a bogus e-mail whose subject or main body contains a topic that seems relevant to the recipient's job, so that the recipients who are interested in it open its attachment (i.e., virus).

If the recipients open such attachment, their PC is infected, possibly leading to information leakage, as well as the distribution of the virus to the corporate network to which the PC is connected, putting the whole company/organization at serious security risks.

Aired Incidents Involving Targeted Attack Mail

- Multiple PCs within the Ministry of Internal Affairs and Communications infected with a virus through "Targeted Attack"
  - A virus posing as an earthquake-related material
- The House of Councilors receives the same "Targeted Attack" as that for the House of Representatives
- "Targeted Attack" against chemical- and defense-related 48 enterprises in the world (including Japan)
- "Targeted Attack" against the ministry of Foreign Affair; infection at some legations abroad; no information leakage confirmed
- A spate of virus attacks against the defense-related industry, damages to eight companies in Japan, the U.S., etc.
- Virus infection at Mitsubishi Heavy Industries, Ltd
  "Leakage of product and technical information not confirmed"
- Staff members' PCs infected with a virus; possible leakage of 886 people's personal information (Shikoku District Development Bureau for the Ministry of Land, Infrastructure and Transport)

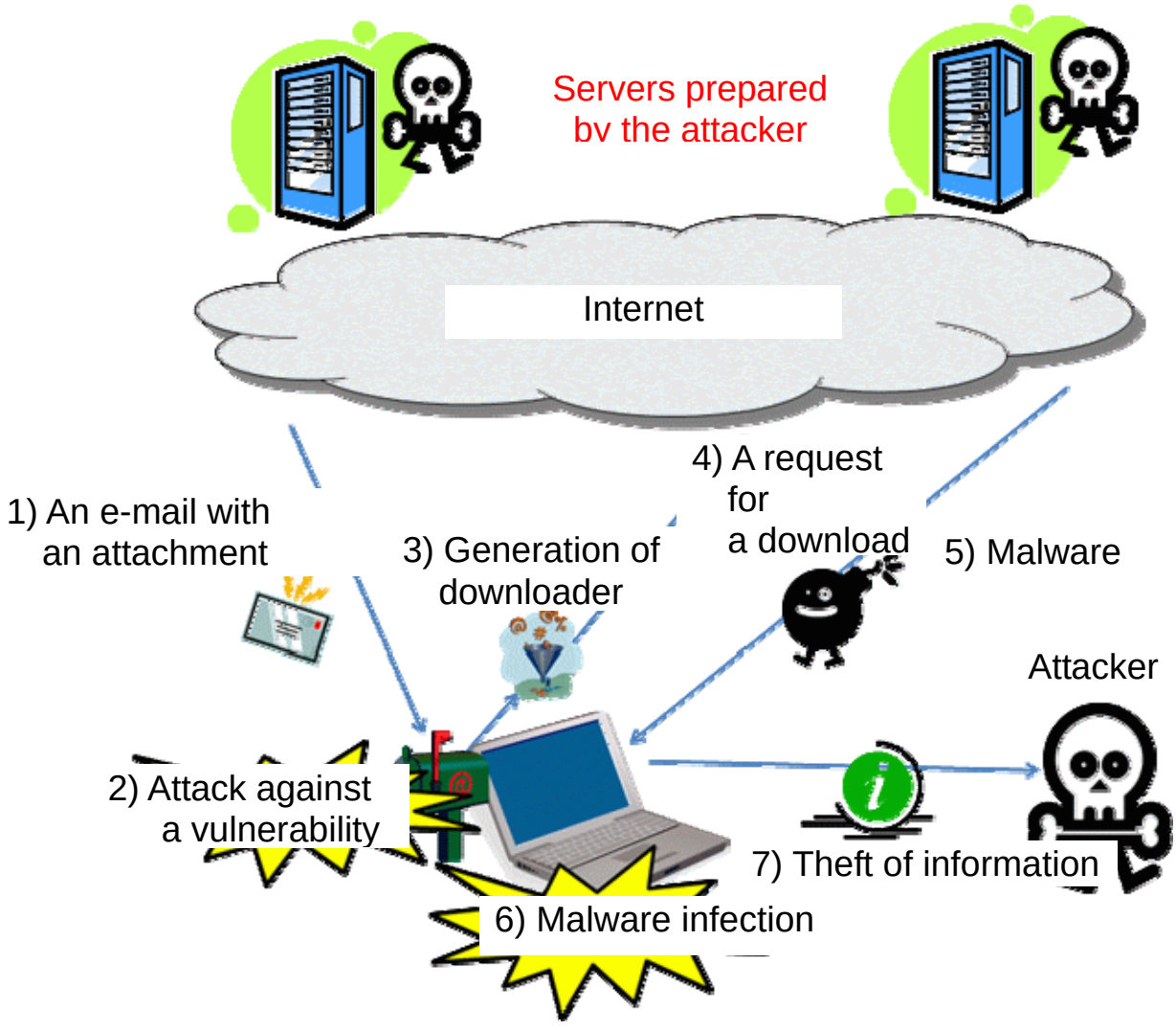
Targeted Attack is on the Rise

- "Targeted Attack" against public institutions or specific companies is on the rise
  (It is highly likely that "social engineering" is used beforehand.)
- Be careful with mail attachments!!
- There are many attacks that exploit vulnerabilities in standard software.
  - **Adobe Reader, Flash Player, Word, Excel, Ichitaro, etc.**
- Infected with Trojan horse by opening an e-mail attachment.
- Once infected, it is difficult to predict what will happen to the PC.

Trojan Horse is Truly Horrible Because:

- **Once it invades (infects) that PC, it downloads other pieces of malware (virus) one after another (i.e., downloader)**
- **It updates oneself (i.e., invalidation of virus definitions)**
- **It attempts to disable antivirus software**
- **It hides oneself (i.e., root-kit)**
- **For business-purpose PCs, if Trojan horse is detected by the antivirus software during its virus scan, it is better to perform initialization (i.e., clean installation of operating system).**

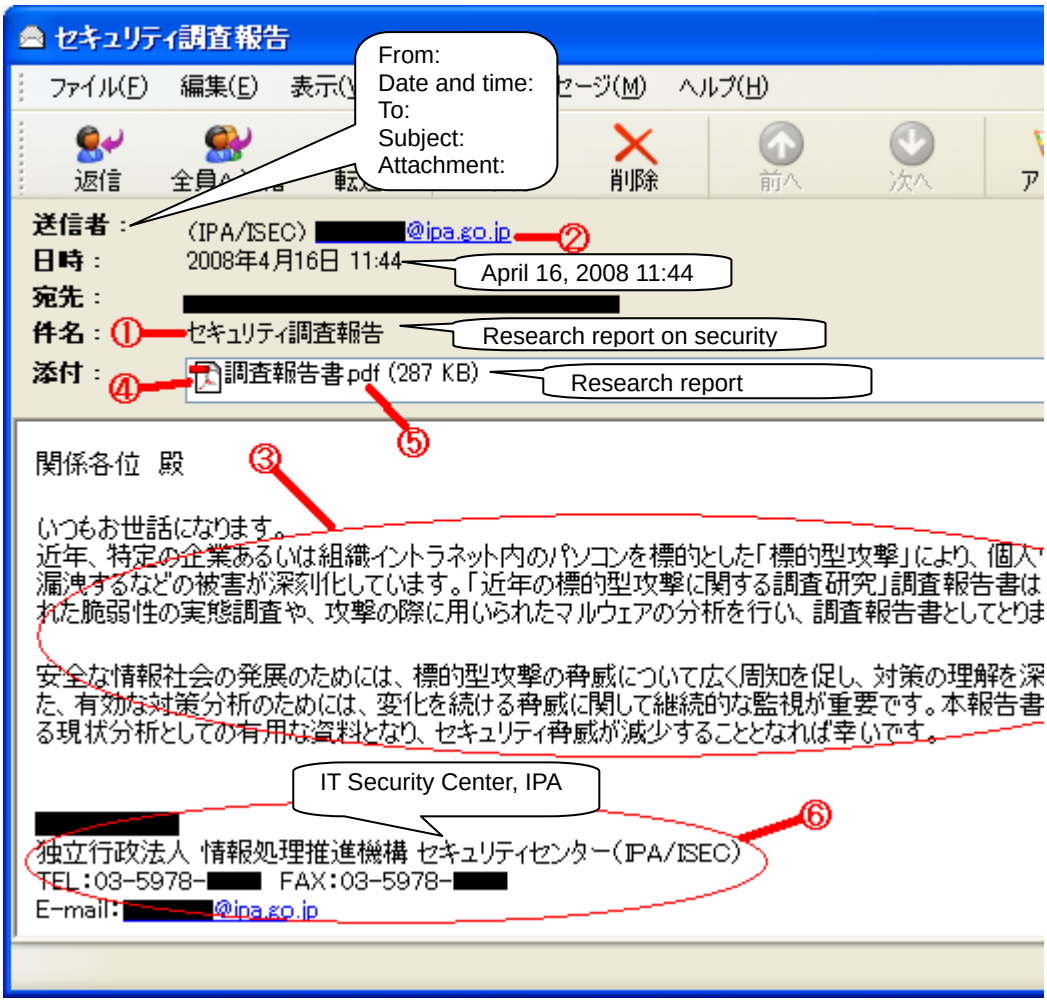
Image of Commonly-Seen, Persistent Attacks by "Targeted Attack"



Incidents of Targeted Attack Mail

One of the characteristics of Targeted Attack mail is: "information posted on a website, etc. is copied into an e-mail's main body, or a PDF report posted on a website is tampered so that it contains a virus", and this has about forty percent in Targeted Attack Mails.

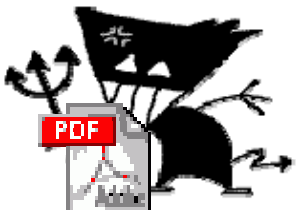
The case below shows a Targeted Attack mail posing as IPA and sent to government-affiliated organizations in April 2008.



This e-mail's main body and PDF file contained the press release information from a report that was posted on IPA's website in March 2008, so the following conditions to deceive recipients were met:

(1) A subject that would attract e-mail recipients' interest;
(2) The sender's e-mail address is that of a reliable organization;
(3) The main body is relevant to the subject;
(4) The attachment's name matches the main body's content;
(5) The attachment is a word processing document or a PDF file;
(6) The signature contains the name of an organization or individual that corresponds to the address described in (2).

This was the case of a Targeted Attack mail posing as IPA (an existing person in charge) and carrying a PDF file tampered to exploit Adobe Reader vulnerability. It was intended to get the recipients to open its attachment (i.e., PDF file) and sent to government-affiliated organizations.



The main body contained some contents copied from IPA's website, and it was assumed that this was done by an attacker having some measure of Japanese.

If the recipients opened this e-mail's attachment by using a vulnerable version of Adobe Reader, their PC was infected with the virus contained.

In fact, this incident was detected owing to some e-mails being sent back to IPA for their unknown destination address. If the recipients had been the people involved in information security and knowing IPA well, they may have been interested in and opened its attachment. At the time of the detection, however, there was no infection report.

In other incidents, an e-mail actually exchanged within a company/organization was abused.

For more details, please refer to the material below.

NB: Since this material is available only in Japanese, we omit it.

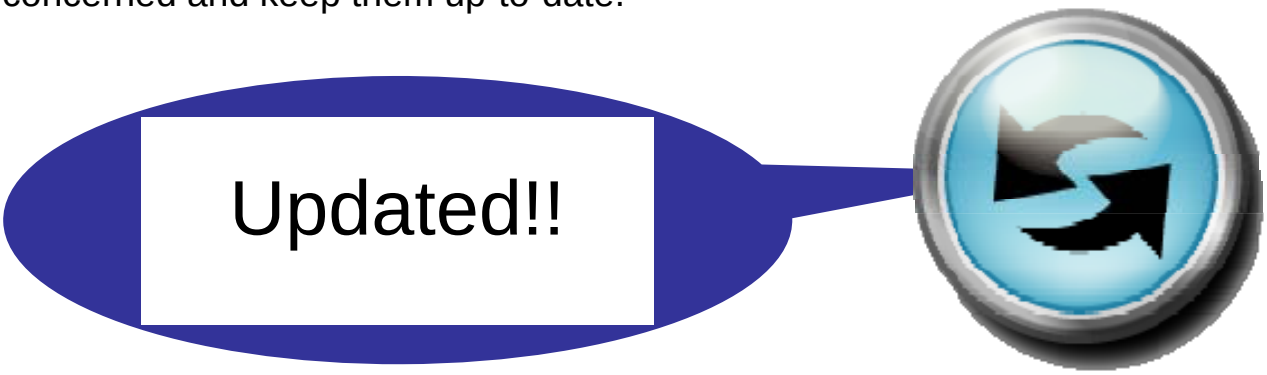
2. Employee Controls

Eliminate Vulnerabilities in Operating System and Applications

According to a survey*[2] by a security vendor Trendmicro, fifty percent of the "Targeted Attack" mails attachments detected so far contained a virus that exploited vulnerabilities in operating system and applications.

So, it is recommended that PC users eliminate vulnerabilities in the operating system and applications on their PC and keep them up-to-date.

Typical applications whose vulnerabilities are often exploited include, as stated earlier, **Adobe Reader, Flash Player, Word, Excel and Ichitaro**. So, the users of these applications need to collect vulnerability information concerned and keep them up-to-date.



For Microsoft OS or Office products (e.g., Word, Excel), you can use Microsoft Update/Windows Update, which is provided as one of OS functions, to bring them up-to-date.

For Adobe Reader, it is recommended to use the **"Check the presence or absence of updates"** function, which is provided as one of the help functions, to regularly check if your Adobe Reader is the latest version. If this check reveals that any update is available, it is recommended to apply it. **For Flash Player**, you can check the version of your Flash Player on the website below (NB: confirmation methods are browser-specific**[3]*); if it is not the latest version, upgrade it to the latest version.

- Adobe Flash Player (A website to check the version in use)
  http://www.adobe.com/jp/software/flash/about/ (in Japanese)

For Ichitaro, visit the website below and apply the Ichitaro update module.

JUST SYSTEM Support Update
http://www3.justsystem.co.jp/download/ichitaro/ (in Japanese)

If any vulnerability is detected in these applications or operating systems or in exploitable applications, information is posted on a site JVN (Japan Vulnerability Notes) run by IPA and JPCERT/CC***4** in collaboration. So, use this site as a reference.

JVN（Japan Vulnerability Notes）
http://jvn.jp/

[Information contained in JVN]
JVN provides a variety of vulnerability-related information collected as well as measures obtained through the coordination with product developers, in an easy-to-understand, organized form. Product developers' response status includes presence or absence of their products having the specific vulnerability, workaround, and countermeasure information such as patching.

*2) Survey by Trendmicro
The material below was released on November 8, 2011.
Monthly report on Internet threats − the October 2011 issue
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20111107015156.html (in Japanese)

*3) Confirmation methods are browser-specific
Adobe Flash Player supports Internet Explorer and other types of browsers (e.g., Firefox). For each browser, it is necessary to visit the aforementioned site and check their version.

*4) JPCERT/CC
JPCERT/CC accepts reports on computer security incidents (hereinafter: "incident") that happen to websites in Japan, including hacking through the Internet and denial of service. It also provides support for incident response, grasps incident status, analyzes the methodology applied, mulls preventive measures and gives advice, from technical standpoint. As a neutral organization which does not belong to any specific government agency or enterprise, it works actively for the improvement of information security measures activities in Japan.

Antivirus Software is Essential

If the malicious code (program) embedded in a Targeted Attack mail's attachment is a known virus, it may be detected by your antivirus software.

And, even if it is not a known virus, if you use antivirus software that has a state-of-the-art "heuristic detection" feature, its malicious conduct may be detected.

For your PC, implement measures to protect against virus infection through a suspicious website or a suspicious e-mail, including installing **antivirus software**.

Furthermore, keep your antivirus software's **virus definition files** up-to-date by enabling **automatic updating**.

Note, however, that antivirus software is not a panacea. **Should you allow for virus infection, settings and information altered or destroyed by the virus might not be restored.** Even if you have installed antivirus software, it does not mean that your PC is totally safe. Overconfidence is big no-no. Use of antivirus software should be considered a precautionary measure. So, don't let your guard down.

Pay Attention to the Attachment's Extension and Attribute

According to the aforementioned survey by a security vendor Trendmicro, fifty percent of the Targeted Attack mails attachments detected so far were executable files (zip-compressed in most cases.)

If fifty percent of Targeted Attack mails attachments are executable files, by checking their extension (or unzipped files'), users may be able to thwart such threat (i.e., the execution of a virus)

Making "a file in executable format" to "a file in another format" getting users to open it is a technique used also for other types of virus infection. So watch out for it!

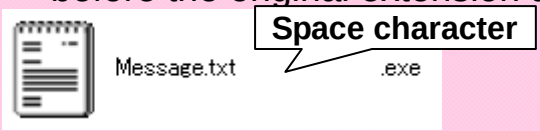
(1) How a File is Disguised

Icon is disguised

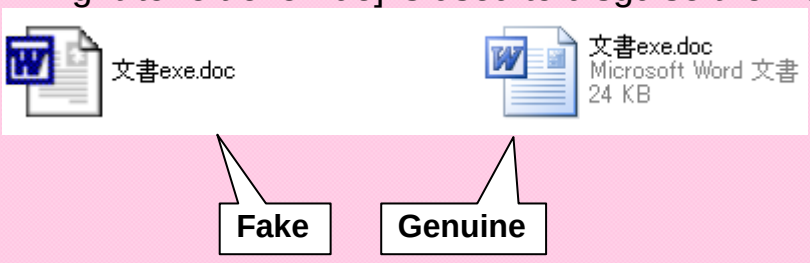
-> Despite being a file in executable format, the icon of a document file/moving image file/picture file is displayed.

File name is disguised

-> Double extension (inserting a string of space characters before the original extension and adding a fake extension)



-> RLO trap (a Unicode control character [RLO：Start of right-to-left override] is used to disguise the file extension)



NB: Fake icons are simplified so that this mechanism is easily understood.

File Attribute is disguised

-> Disguises file attribute through the exploitation of "Hide extensions" (which is a folder option of Microsoft Explorer);
-> Disguises self-extracting compressed files;
-> Diverts users' attention by displaying a message (e.g., "Encrypting …") and prompting them to perform some sort of operations;
-> Files before compression may also be disguised, so caution should be exercised (NB: also with decompressed files)

Furthermore, a sophisticated disguise with a combination of these is also possible.

(2) How to See through Disguised Files

It is dangerous to easily open an executable file attached to an e-mail.

The quickest way is to **check with the sender**. If the sender is your acquaintance, by using phone or other means, ask him/her if he/she actually sent that e-mail with that attachment.

If you fail to contact the sender:

- For an attachment which you think needs to be verified, move it to the folder for the verification (NB: if needed, decompress it by using compression/decompression software);
- Next step is **to check the file's attribute (property)** (For Windows OS, put your mouse pointer over the file name, right-click it and select "Property" from the menu);
- If it seems that the file's property is disguised, do not open the file;
- **If you cannot make your own judgments, consult security professionals such as your system administrator.**

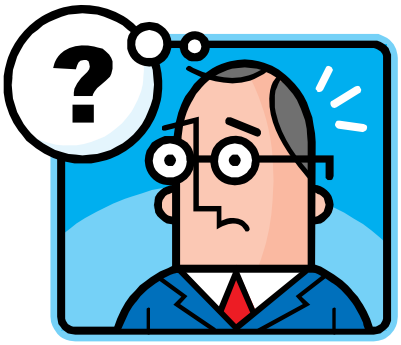
For more details, please refer to "IPA Countermeasures Guide Series **(1) Countermeasures on Computer Virus**".
http://www.ipa.go.jp/security/antivirus/shiori.html

Pay Attention to the E-mail's Sender and Contents

If you find anything unnatural (e.g., the e-mail is from a person with whom you do not regularly exchange e-mails; the e-mail's contents seem irrelevant to the sender; or the sender's name and the signature are not identical), caution is needed. When feasible, check with the sender.

If you cannot make your own judgments, again, **consult security professionals such as your system administrator**. Remember that a selfish (halfway) judgment may cause too much trouble to your company/organization.

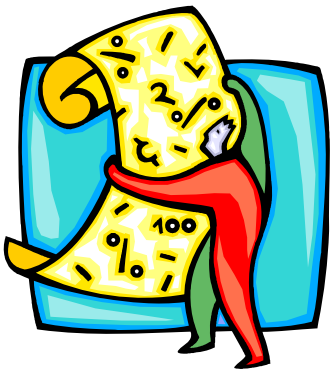
(1) For Example, Watch out for an E-mail Described Below!!



- The subject or main body contains bumbleheaded Japanese phrase (automatic translation?);
- The e-mail is from an unknown individual/ company;
- The contents are irrelevant to your business operation;
- Obviously, the e-mail's contents are designed to have the recipients open its attachment;
- The subject contains an exaggerated keyword (e.g., [Important Notice], [Urgent], [Express], [Important].)

(2) Measures below are also Effective

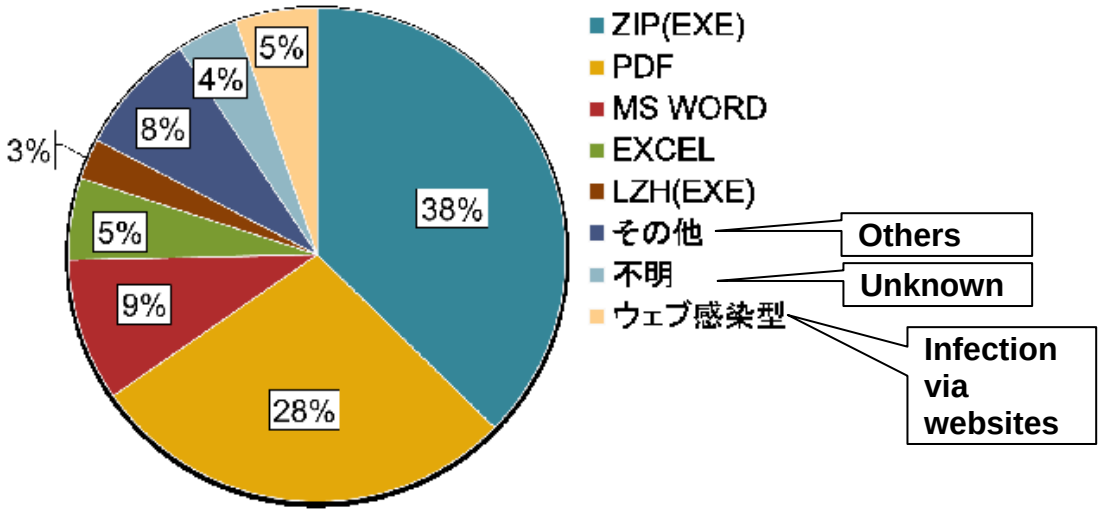
- Making use of signature, ranging from a simple signature to fingerprint (to guarantee the contents) or electronic signature (to authenticate the sender)
- Working out an arrangement about secret language with an individual/company with whom you regularly exchange e-mails.



Just for Information（Reports and Inquiries to IPA）

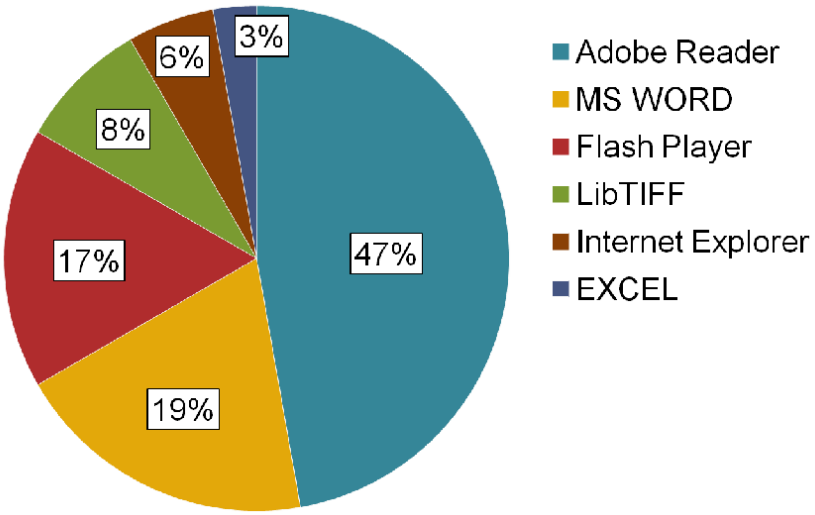
Based on the reports and inquiries made to IPA, we calculated a sum for each type of Targeted Attack mails attachments. The breakdown is shown below.

When IPA began to provide consultation about Targeted Attack mails, "exe" files or "zip" files (i.e., "exe" files being zip-compressed) were mainly used for mass-mailing type viruses, while document files such as MS Word/Excel files and PDF files were mainly used for Targeted Attack mails. But nowadays, zip files obtained by zip-compressing "exe" files are on the rise.



The next is the breakdown of applications whose vulnerabilities were exploited.

Most of such document files were designed to exploit vulnerabilities in Adobe Systems' products.



Both of the data show the same trend as indicated by the aforementioned survey by Trendmicro.

3. Organizational Measures

Countermeasures against Social Engineering

An attacker who carries out Targeted Attack may implement social engineering*5 first against the target company/organization. This is exactly a preliminary survey to successfully carry out Targeted Attack, and it is obvious that a company/organization whose security measures are loose can easily be targeted (Broken Windows Theory*6).

For example, there was a case of Targeted Attack mail in which an e-mail actually exchanged within a company/organization was abused. If an actually-used e-mail is abused, the recipients are more likely to open it unsuspectingly. If you send an e-mail to a wrong address, or if your e-mail is intercepted by some means, or if you carelessly post critical information on SNS etc., it might by abused by an attacker. Wrong transmission of e-mails and transmission/reception of critical information in plain text (i.e., an act of including critical information in the body text) is pretty dangerous. Apart from them, a security incident that causes e-mail addresses of people concerned to be leaked is also dangerous. Because a Targeted Attack mail may be sent to the people concerned, posing as the company/organization that leaked the information.

As for social engineering, a company/organization or a fake system administrator asking employees' account information over the phone has been famous since former days. In that sense, it is dangerous to carelessly dispose of information (paper or electronic media). Furthermore, it is also dangerous to carelessly respond to unnatural inquiries.

Companies/organizations need to make their employees aware of these problems and to regularly provide education and training for not causing security incidents.

*5) Social engineering
An act of obtaining classified information such as password by exploiting human psychology or by unexpected means, without using network technology or computer technology. Examples include: cheating to get password with verbal dexterity, reading out critical information from waste materials, peeping and eavesdropping by disguising as an employee. This is also called social hacking or social cracking.

*6) Broken Windows Theory
This theory is: "In the case of a building that has a broken (yet not renewed) window (NB: since this is a building with sloppy management, anticrime measures should also

be loose …), someday, all other windows may also be broken (i.e., easily targeted by burglaries)."
For the same reason, a company/organization whose information security is loose would easily become the target of a cyber-attack.

Providing Training on Security Rules and Having Employees Follow Them

As with countermeasures against social engineering, it is important to provide employees with training on security rules that comply with the security policy established by the company/organization and to have employees follow them.

To protect ourselves from Targeted Attack at the border, it is necessary for all the employees to have unified security awareness (i.e., to have the same problem consciousness against Targeted Attack). Make them aware of the fact that, a single person's carelessness may cause a company/organization-wide problem.

In particular, for the measures described in the "Employee Controls" section, it is recommended to make them rules and provide education and training.

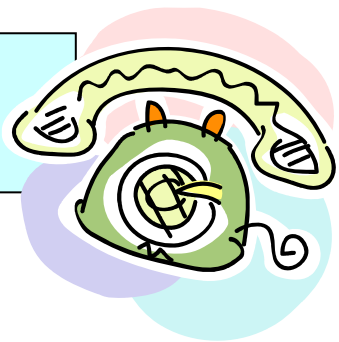
Information Sharing

In most cases, Targeted Attack takes a shot at a specific company/organization. If you receive any suspicious e-mail, let's share the information swiftly. By doing so, we can prevent the damage from spreading.

To prevent further damages by Targeted Cyber-Attacks, Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) was established on October 25, 2011. It was founded under the supervision of the Ministry of Economy, Trade and Industry and mainly composed of critical infrastructure equipment manufacturers (such as in the heavy industry and the field of heavy electric machinery), aiming at promoting information sharing and swift response, and the "Special Consultation Service for Targeted Cyber-Attacks" was also set up within IPA.

The "Special Consultation Service for Targeted Cyber-Attacks" answers inquiries about Targeted Attacks, anonymizes information, and shares information with partners. If you find any Targeted Attack mail that may affect not only your company/organization but also other companies/organizations, please provide that information to the contact address below.

Special Consultation Service for Targeted Cyber-Attacks
TEL: 81-3-5978-7509 FAX: 81-3-5978-7518



Settings for the E-mail Server

For e-mail servers used by companies/organizations, it is important to make settings so that executable files cannot be attached to e-mails or that executable files attached to incoming e-mails are isolated.

Recall the report that fifty percent of Targeted Attack mails attachments are executable files … (See page 9 in this guide.)

Furthermore, such settings should be communicated to all the employees, along with the reality of Targeted Attacks.

Settings for Filtering

Trojan horse (virus) downloads many different malicious programs from the Internet (See page 4 in this guide.) And so, filtering websites so that employees cannot access any irrelevant websites is effective in preventing the entry of malicious programs by Targeted Attacks.

Applying such website filtering may impair information-gathering activities and marketing activities, but employees should be aware of the fact that, filtering is necessary to protect themselves from Targeted Attacks.

Physical Controls

As stated in "Introduction", this guide is written for company/organization employees. Therefore, this guide does not provide the details of the physical controls that should be implemented by the System Management Department within companies/organizations.

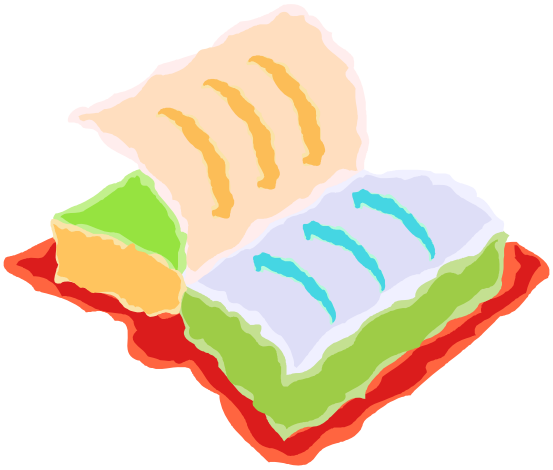
For the information on the physical controls that should be implemented by companies/organizations against Targeted Attacks, refer to the material below.

- **Design and Operational Guide to Cope with "Advanced. Persistent Threats"**
  http://www.ipa.go.jp/security/vuln/newattack.html

4. Reference Information

<IPA>

- **Design and Operational Guide to Cope with "Advanced Persistent Threats", released**
  http://www.ipa.go.jp/security/vuln/newattack.html



IPA Countermeasures Guide Series

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA Countermeasures Guide Series **(1) Countermeasures on Computer Virus**
- IPA Countermeasures Guide Series **(2) Countermeasures on Spyware**
- IPA Countermeasures Guide Series **(3) Countermeasures on Bots**
- IPA Countermeasures Guide Series **(4) Countermeasures on Unauthorized Access**
- IPA Countermeasures Guide Series **(5) Countermeasures on Information Leakage**
- IPA Countermeasures Guide Series **(9) Guide for First-Time Information Security Countermeasures**
- IPA Countermeasures Guide Series **(10) Countermeasures against Targeted Attack Mail**

Information-technology Promotion Agency, Japan
IT Security Center

Bunkyo Green Court Center Office 16th Floors
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan 113-6591

URL **http://www.ipa.go.jp/security/**

[Worry-Free Information Security Consultation Service]

URL **http://www.ipa.go.jp/security/anshin/**
E-mail **anshin@ipa.go.jp**