18th Annual FIRST Conference
June 25–30, 2006
Renaissance Harborplace Hotel
Baltimore, Maryland USA

JPCERT/CC™

Threats of P2P File Sharing Software

-- a Japanese Situation About "Winny"--

JPCERT/CC is an independent non-profit organization, acting as a national point of contact for the other CSIRTs in Japan. Since its establishment in 1992, the center has been gathering computer incident and vulnerability information, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues.

Keisuke Kamata

Yuichi Miyagawa

JPCERT Coordination Center

Japan

Goals And Objectives

This presentation should:

- Provide good understanding of the “Winny” and the situation in Japan.
- Be a trigger to considering the information leakage incidents.

Topics

- P2P file sharing software “Winny”
- History of “Winny”
- Information leakage incidents and reaction/response
  - Japanese government
  - media
  - IT professionals
- What was these incidents really told ?

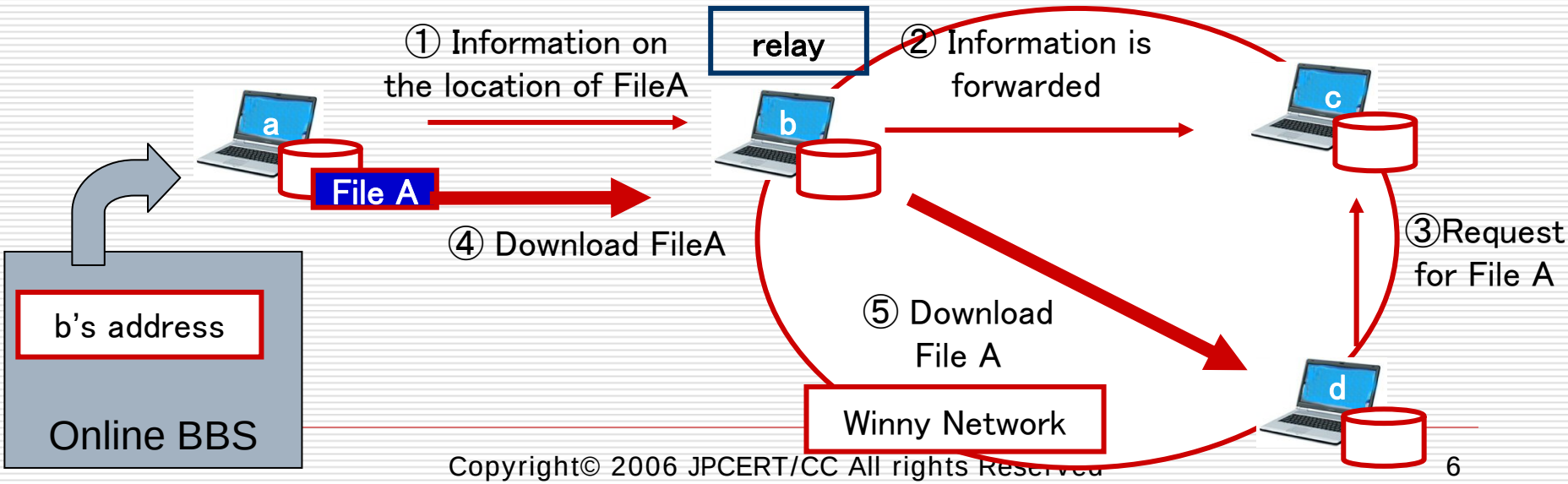
Winny Technical Details

P2P File Sharing Software in Japan

- Napster
  - Central server has file lists.
- GNUTELLA
  - Publish the IPs on website.
- WinMX
  - Napster + GNUTELLA like
- Kazaa
  - concept: Super Node & Ordinary Node
  - VoIP software “skype” uses this technology
- Winny (Japanese)
  - Pure P2P type, anonymity, cache mechanism
- share (Japanese)
  - Winny + spreading upload mechanism

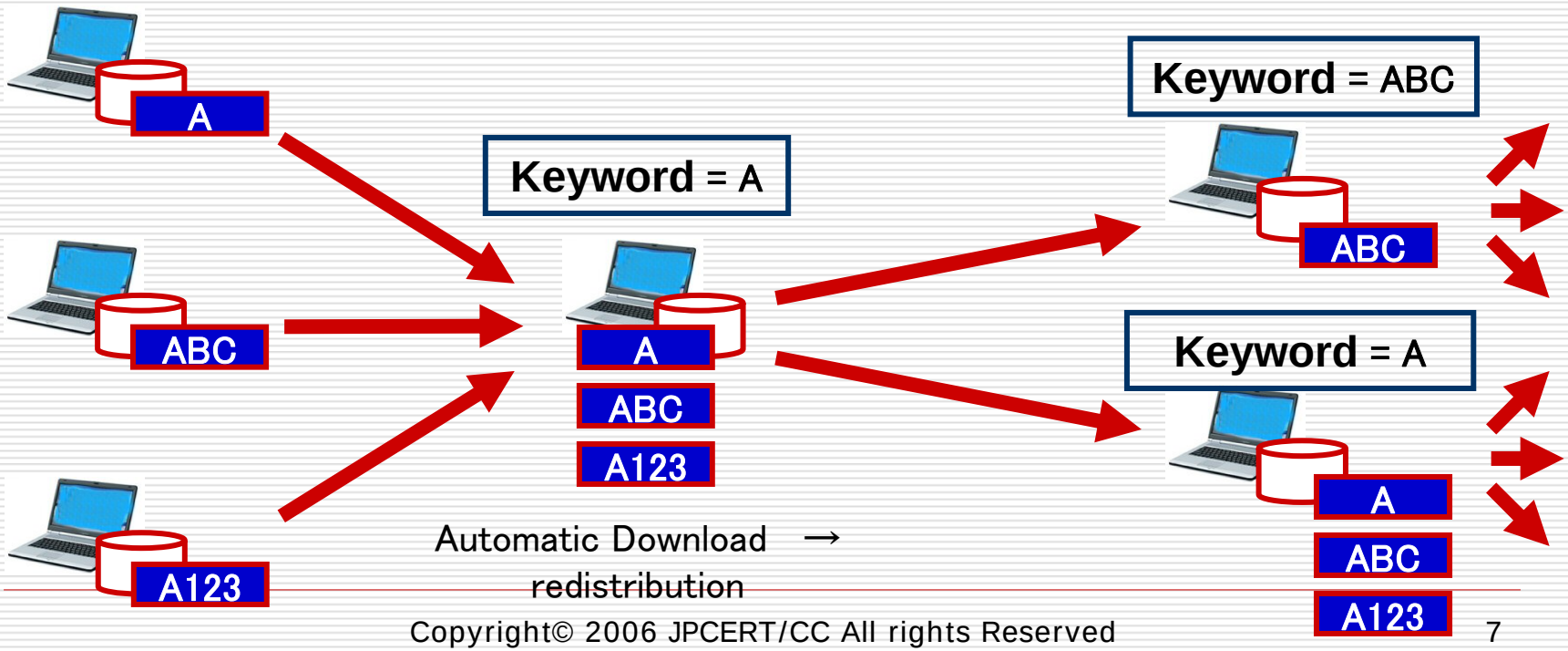
Pure type P2P

- No Index server
  - There is no central server managing the network. All functions such as file search and file transferring are constructed only by the PCs in the network.
  - Users join by acquiring the initial node online, typically BBS.
- Impossible to manage
  - Even the creator has no way of grasping what is going on in the whole system.
  - There is no effective means of controlling or stopping the flow of contents within the network.



Auto downloading and re-publish

- Files are automatically downloaded upon keyword match.
  - User intentions do not interfere with this action
- Contents are cached, and then redistributed in the system.



Other Features

- Anonymity
  - Multi-hop proxies and re-exhibition of cached contents.
  - Encryption
  - Automatic selection of connecting PC.
- Built-in measures for efficient expansion
  - Clustering of PCs by keywords.
  - Multiple downloads.
  - Automatic adjustment of file transferring speed.
- User convenience
  - Posting fake-content warnings.
  - Version-up alerts
  - Filtering download contents by keywords.

Typical action of a Winny user

1 Access	2 Set keyword	3 Working	4 Check	5 Save
Get up ☐Start Winny. ☐Access to the Winny network.	**Before going to Work** ☐Set a favorite movie's title for the search keyword. ☐Leave Winny on while at the office.	At the office ☐Winny automatically downloads and saves files that match the set keyword.	Back at home ☐**Open and check the files that Winny has downloaded.** ☐**Delete crashed files and unneeded files.**	Go to bed ☐Save and backup the files you liked.

Actions in step 4 became target of viruses

Virus Detail

Summary of Antinny

- Spread in mid 2003.
- A “Trojan horse” virus that spread via Winny.
- Leaks information, deletes files, does DDos, etc.
- Over 50 similar derived viruses.
  - Viruses are designed to be executed by the user, therefore does not require special knowledge (such as designing attacks on vulnerabilities) and is easily created.
- Over a 170,000 PCs were confirmed to be infected.

- Information leaked from companies, autonomies, and individuals causing serious social problem.

The distinctive actions of an Antinny virus

- Being automatically downloaded.
  - Uses a popular keyword for its file name.
  - Is often downloaded and re-distributed, therefore spreads widely quickly.
- Uses the user's habitual action of checking all downloaded files to make the user execute itself.
  - Packages itself together with contents in a zip
  - Changes its icon into a word or folder icon.
  - Changes its file name so that the extension is hidden

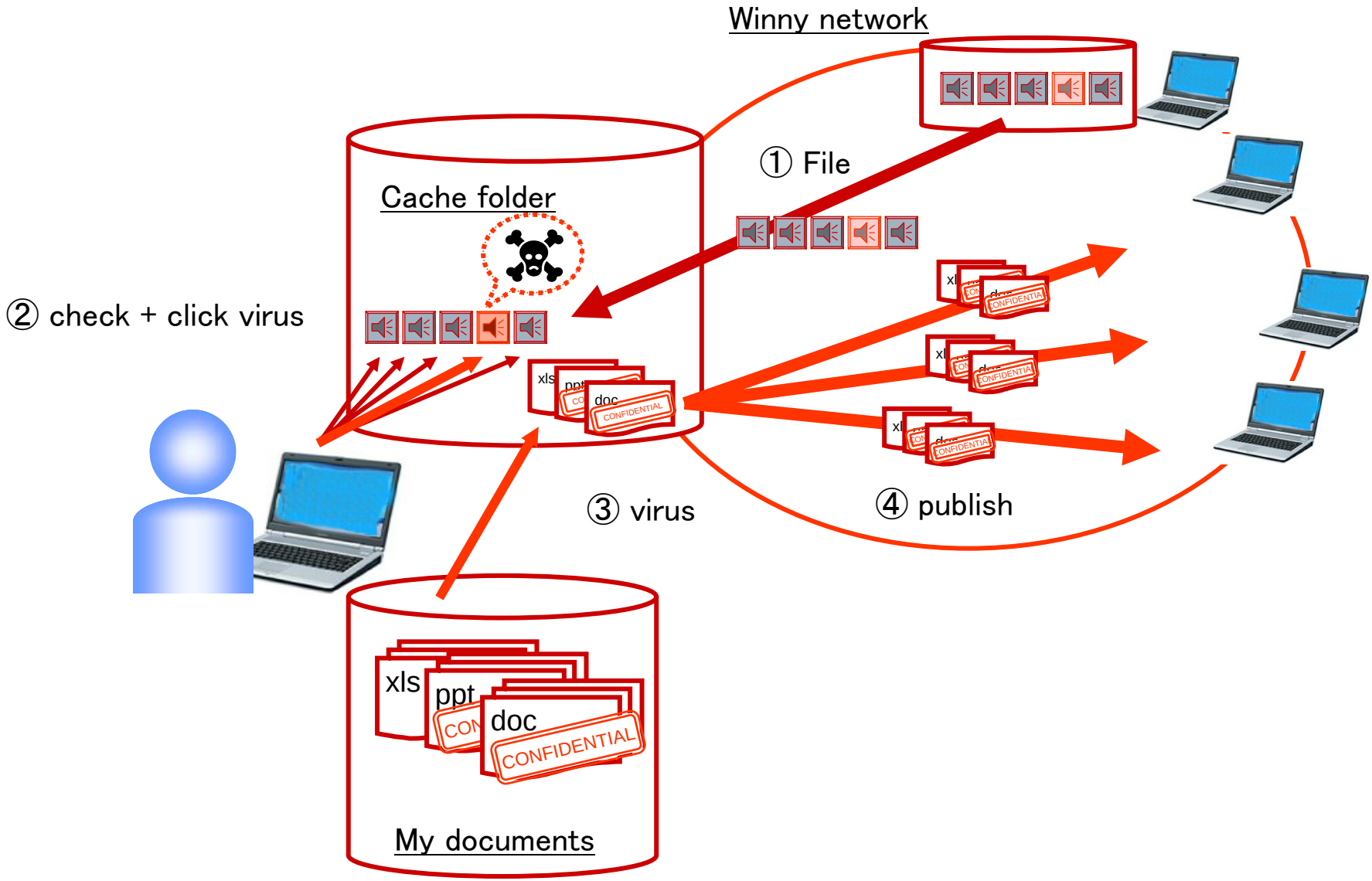
  e.g.) StarwarsⅢThe Complete Edition .exe

- Makes the user unaware of the infection.
  - Pops a fake message (e.g. This file is broken)
  - Shows a dummy HTML file.

An Example of an Infection

1. The user executes the virus (details shown later)
    1. Takes advantage of the aforementioned “checking” action.
2. Shows a message such as “This file if broken.”
3. Actions upon infection
    1. Re-distributes itself at Winny network.
    2. Distributes doc .xls .dbx .ppt .txt .pdf files that saved on PC.
    3. Changes Windows registory so that it automatically starts-up.
    4. Regularly captures the desktop image and distributes it.

Office documents, e-mails, photos, etc...
were distributed at Winny network


Winny network
① File
Cache folder
② check + click virus
xls
ppt
doc
CONFIDENTIAL
③ virus
④ publish
My documents

History of “Winny”

May 2002

- Project has started and declared on huge BBS website called “2ch”
  - Win MX → Win NY (M→N、X→Y)
  - some WinMX users arrested
  - winny’s concept is “anonymity”

November 2002

- Japan Self Defense Force's internal document was leaked to the "Winny network"
- It is recognized it's unlikely to be caused by "Worm" or "Virus"

May 2003

- Winny2 beta was released
  - **no protocol compatibility**
  - **no setting compatibility**
  - **cache compatibility**

August 2003

- ぬるぽワーム (nu ru po Worm)
  - named Antinny.A
  - Written in Visual C++
  - Displays fake message when executed
    - “The folder is not available or broken”

November 2003

- **The ISP “Plala” started to restrict “WinMX” and “Winny” traffic.**
  - bandwidth problem

November 2003

- Kyoto local police arrested two users.
  - Because of distributing PC games and Movies illegally.
  - breach of the Copyright Act
- Winny developer's house was searched by police.
  - source code of "Winny" was seized

April 2004

- **Symantec released an alert on new worm “Antinny.G”**
  - **Antinny.G leaks the infected user’s information to ACCS**
    - **ACCS is “Association for Copyright of Computer Software “**
  - **Copy some files to Winny upload folder.**

May 2004
DDoS attacks to ACCS

- Antinny.G attacks to ACCS webserver
  - 700Mbps of DDoS attack on Sep/9/2004
  - ACCS changes the domain name
  - Antinny.AX attacks to the new domain

May 2004

- Kyoto local police arrested Winny developer
  - aiding of copyright violation
  - University researcher
  - age 33

October 2004

- New virus has appeared
  - upload “desktop screenshot” to Winny network
  - upload filename is include: [My Desktop]
  - upload “My favorites”
  - upload e-mail
  - “desktop screenshot” leaks regularly

February 2005

- 欄検眼段 (Ryan Ku Gan Do)
  - upload digital photos to Winny
    - search “DSC*.JPG” files in HDD
  - looks like commercial application installer when executed

Information leakage incidents

- Atomic power plant's documents
- Primary school's students info
- Patient's carte
- Cell phone customers info
- Insurance customers info
- First food customers info
- Anti virus vendor's customer info
- Citizens info
- CATV users

and 100+ information leakage was happen...

Reactions

- Microsoft released Antinny removal tool
- Many other vendors also released some tools to detect/delete/stop “Winny”
- Some ISP restrict “Winny” transaction
- Security vendor releases IDS signature
- Many Japanese media (TV/newspaper) bring up the issue
- director of the cabinet secretariat announced “Do not use Winny in this situation” on TV

What was really a problem ?

- People installed “Winny” to a business use laptop.
  - confidential documents were installed in the machine
- Information leakage is a risk management problem.
  - It is not only technology side problem

Important things

- Organization Policy
- Technology
- Information Governance
- Staff Education and Awareness

Contact:

- JPCERT Coodination Center
  - Email：office@jpcert.or.jp
  - Tel：+81-3-3518-4600
  - http://www.jpcert.or.jp

- Watch and Warning Group
  - Email：ww-info@jpcert.or.jp

Fingerprint ：470F F413 3DCC 5D38 7CAC 3500 80C4 944B 298F 386F

Thank you !!