Microsoft Print Spooler Service Impersonation Vulnerability

MS10-061

2010/09

Willy Chang, 2013/04/09

Affected Systems (Both 32/64bit)

- Remote Code Execution:
  - Windows XP SP3 (all lang.)
- Privilege Promotion
  - Windows Server 2003
  - Windows Server 2008 / 2008R2
  - Windows Vista
  - Windows 7

Key Point

- File and printer sharing service
  - → Open port 445 for microsoft-ds service

- Loose Print Spooler Service Authentication

Most known application

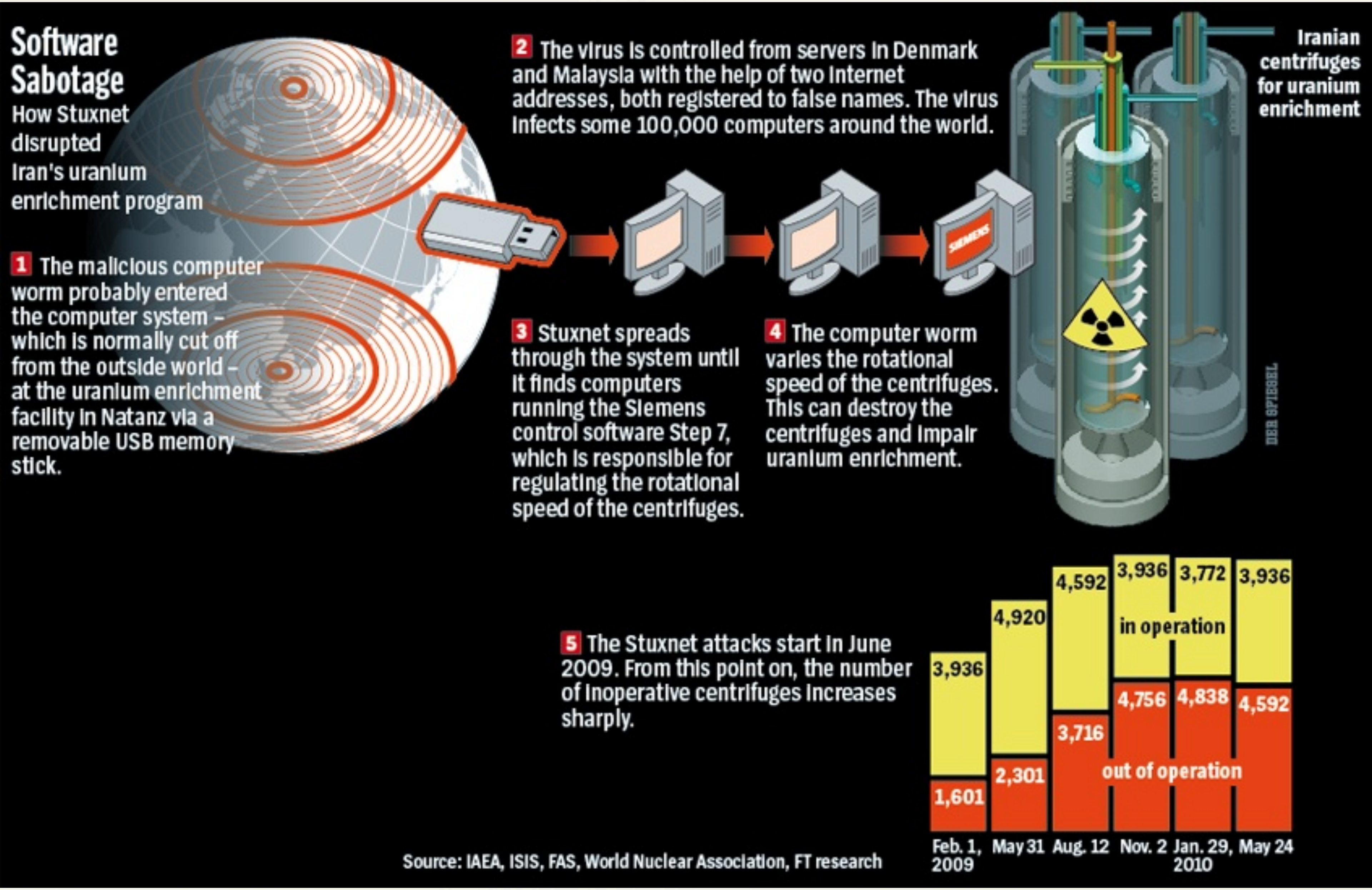
- Worm Stuxnet (2010/6)
  - “The ‘Best’ Malware ever ”
  - Combination of
    - `MS10-046` (Link shortcut parsing)
    - `MS08-067` (RPC Calling Buffer Overflow)
    - `MS10-061`
    - **Rootkit**

    And others.

Stuxnet

- First worm that do little harms to personal system.

- Targeted to Iran's nuclear facilities and Siemens’ SCADA(工業用資料採集系統)



Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

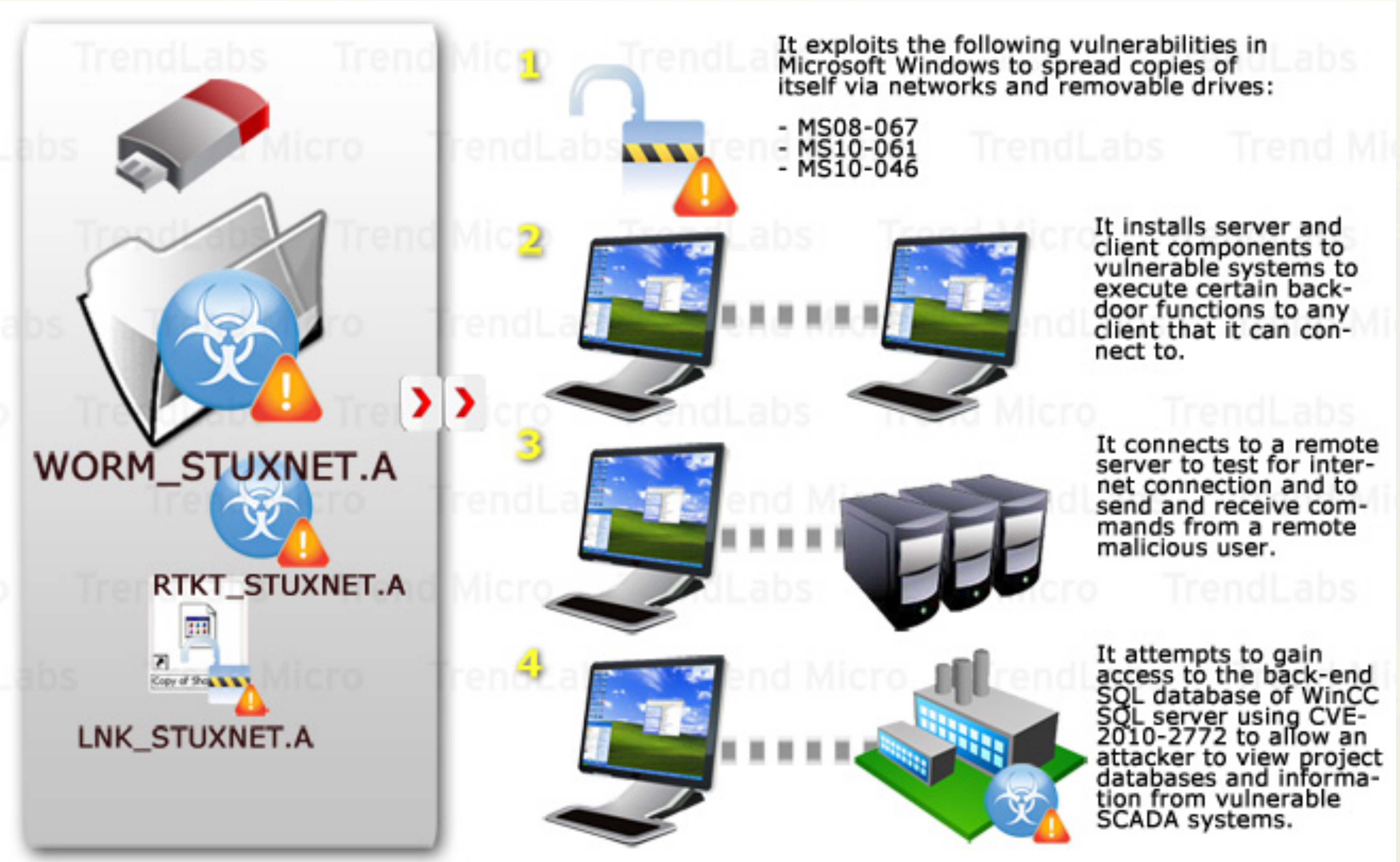
2 The virus is controlled from servers in Denmark and Malaysia with the help of two internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research



1 It exploits the following vulnerabilities in Microsoft Windows to spread copies of itself via networks and removable drives:

- MS08-067
- MS10-061
- MS10-046

2 It installs server and client components to vulnerable systems to execute certain back-door functions to any client that it can connect to.

3 It connects to a remote server to test for internet connection and to send and receive commands from a remote malicious user.

4 It attempts to gain access to the back-end SQL database of WinCC SQL server using CVE-2010-2772 to allow an attacker to view project databases and information from vulnerable SCADA systems.

TrendLabs Trend Micro

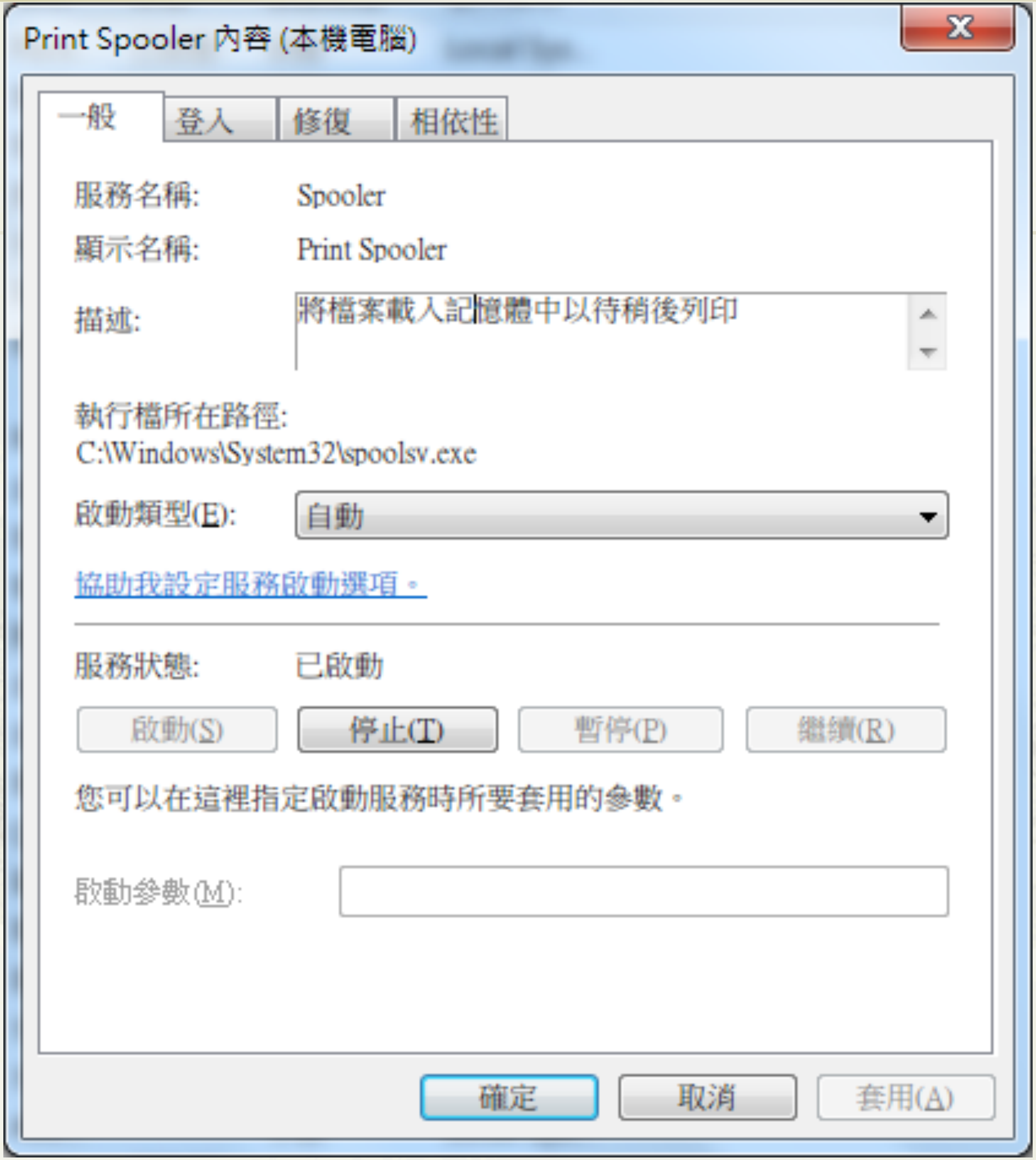
NOW YOU KNOW
A **TINY CRACK** OF AN EGG CAN EASILY **DESTROY A FULL ONE.**

SO HOW DID IT WORK?

Print Spooler Service

- A system service that provide multiple printers to spool the queued documents.

- Automatically started and essential
  - Stop it and generally all the printers get down



服務名稱: Spooler

顯示名稱: Print Spooler

描述: 將檔案載入記憶體中以待稍後列印

執行檔所在路徑:
C:\Windows\System32\spoolsv.exe

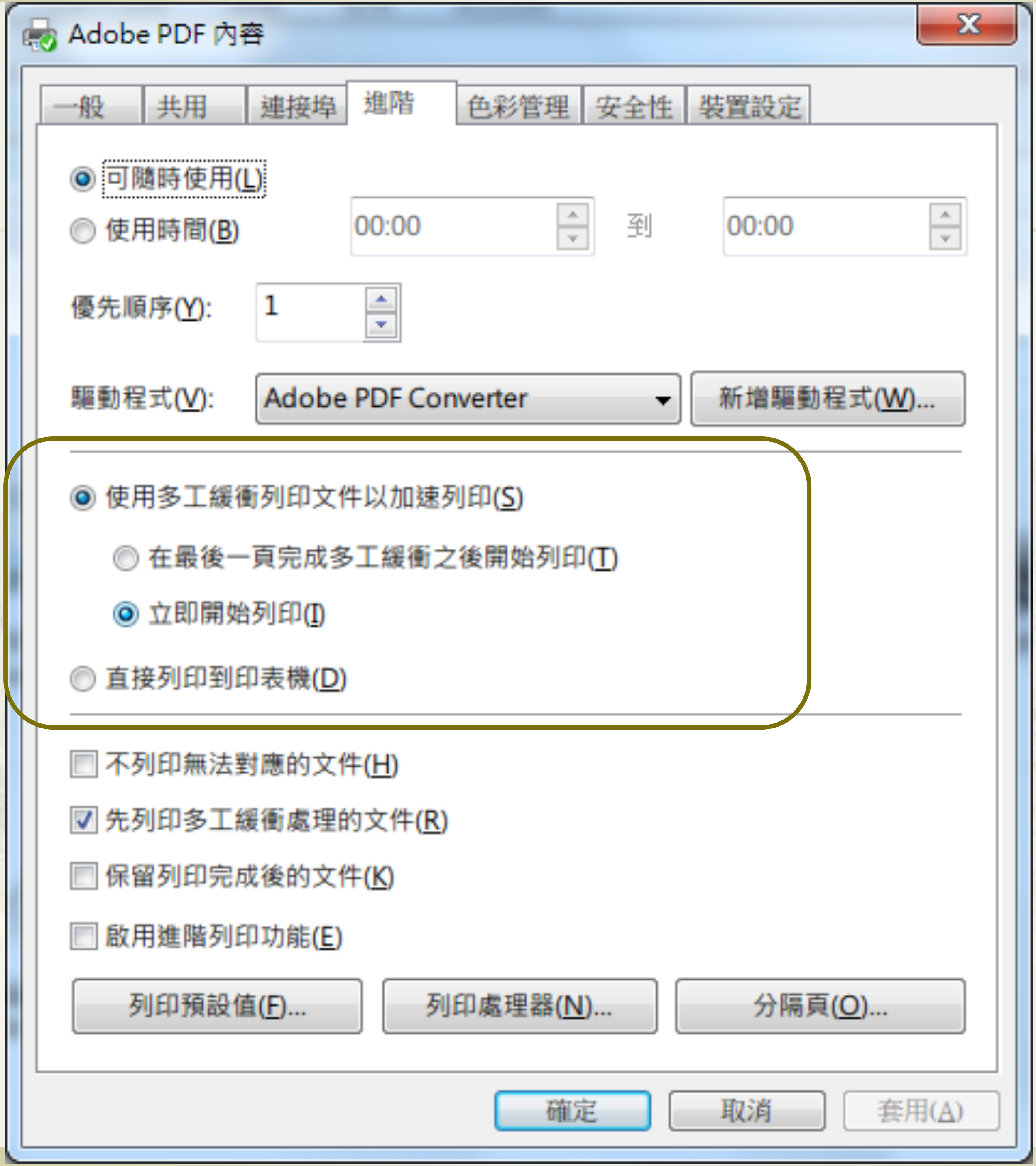
啟動類型(E): 自動

協助我設定服務啟動選項。

服務狀態: 已啟動

您可以在這裡指定啟動服務時所要套用的參數。

啟動參數(M):



Adobe PDF 內容

● 可隨時使用(L)

○ 使用時間(B) 00:00 到 00:00

優先順序(Y): 1

驅動程式(V): Adobe PDF Converter

● 使用多工緩衝列印文件以加速列印(S)

○ 在最後一頁完成多工緩衝之後開始列印(T)

● 立即開始列印(I)

○ 直接列印到印表機(D)

□ 不列印無法對應的文件(H)

☑ 先列印多工緩衝處理的文件(R)

□ 保留列印完成後的文件(K)

□ 啟用進階列印功能(E)

Concepts

- Find a pre-shared printer
- Send a “document” for printing
- `_YstartDocPrinter()` handle the printing event and **select output WITHOUT proper privilege checking**

```
DWORD StartDocPrinter(
  in HANDLE hPrinter,
            //Printer handler
  in DWORD Level,
            //pDocInfo Structure Version, should be 1
  in LPBYTE pDocInfo
            //Pointer to the document info structure
);
```

```
typedef struct _DOC_INFO_1 {
   LPTSTR pDocName;
            //Document name to be printed
   LPTSTR pOutputFile;
            //Full path of the output document.
            //NULL if output by printer
   LPTSTR pDatatype;
            //Data type of the document.
} DOC_INFO_1;
```

Concepts

- Via the assignment of `pOutputFile`, a user could output `pOutputfile` to the system.

- Because of lack of `_YstartDocPrinter()` of privilege checking,

  - One with ANY PRIVILEGE can output ANY FILE to ANY directory.

- Send crafted request to system path and execute → OWNED!

Implementation

- Using BT5 to send fake request
- The “document” to send : PAYLOAD `reverse_tcp`
  - To create a reverse TCP link back to host server for remote controlling
- Directory to output : `%SYSTEM%`
  - `Default>> X:\WINDOWS\SYSTEM32`

Expected Result

- Getting control to the victim with `NT_AUTHORITY\SYSTEM` privilege. (HIGHEST)

Demonstration

- Host:
  Backtrack 5 R3
  - Linux 3.2.6
- IP : 192.168.1.83/24

- Victim :
  Microsoft Windows XP SP3
  - Windows 5.1.2600.5512
- IP : 192.168.1.85/24

Patch?

- Hotfix KB2347290 solved this vulnerability.
- Windows 6.1 SP1 included

- Now before output, two function is called :
  - `CheckLocalCall()`:
    Check if caller has local administrator privilege
  - `ValidateOutputFile()`:
  - To check if output creation is prohibited

YOU’RE NEVER BEING HEALTHY UNTIL IT’S FOUND.

GO INSTALL PATCHES AND STAY UPDATED.