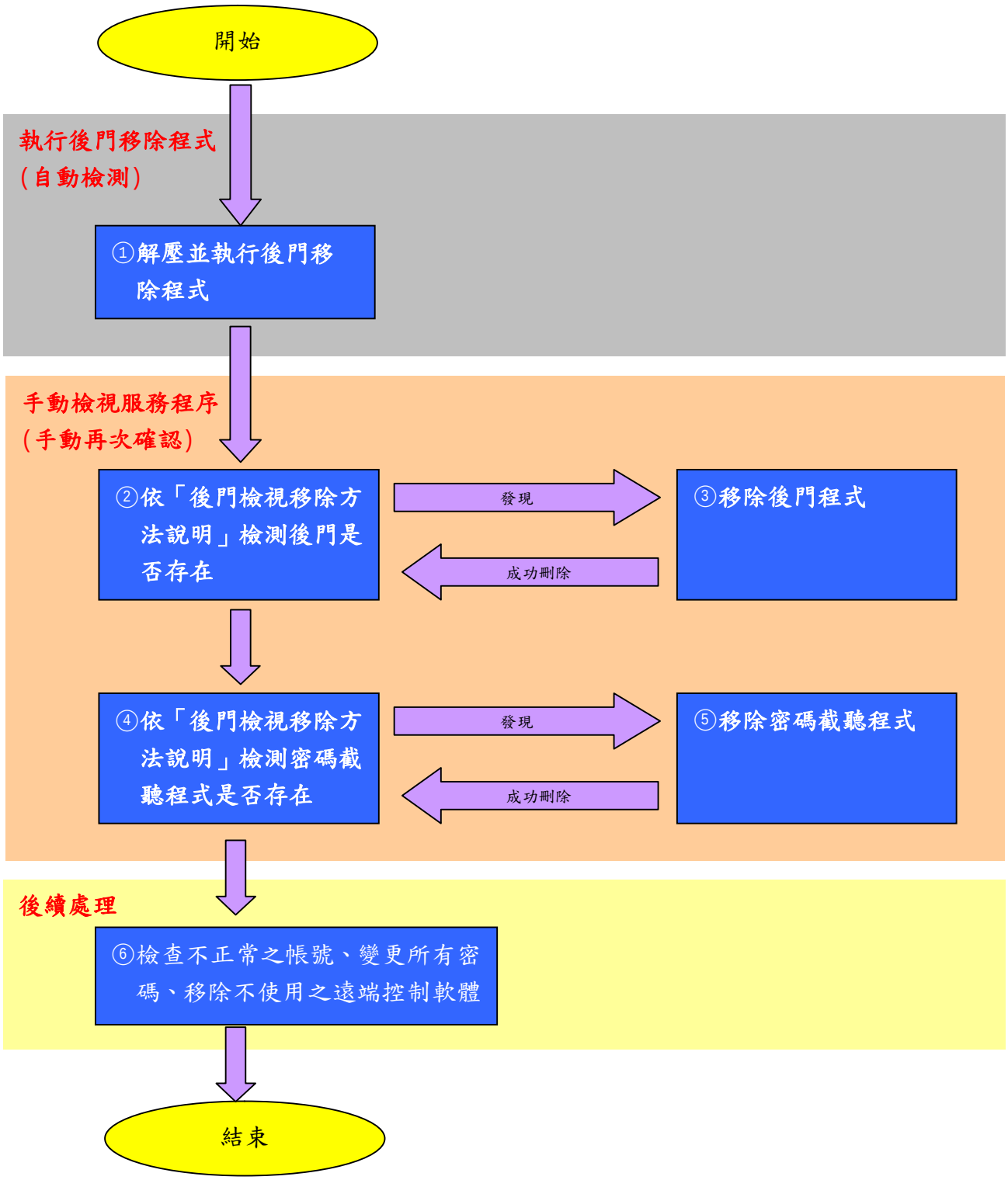
後門移除 SOP

一・ 後門移除流程

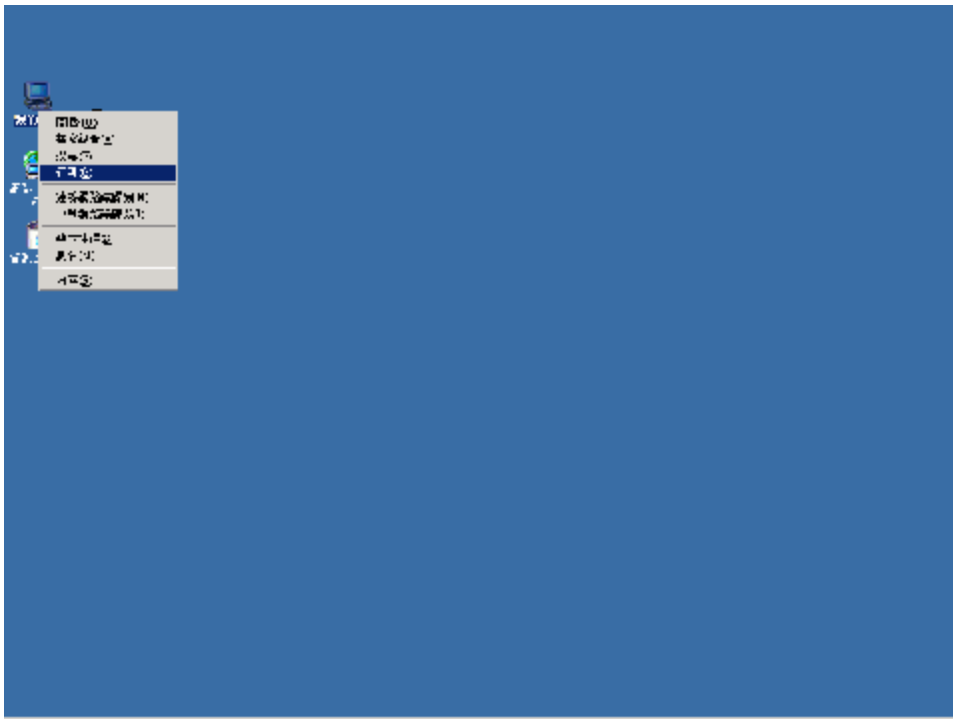


二・後門檢視移除方法說明

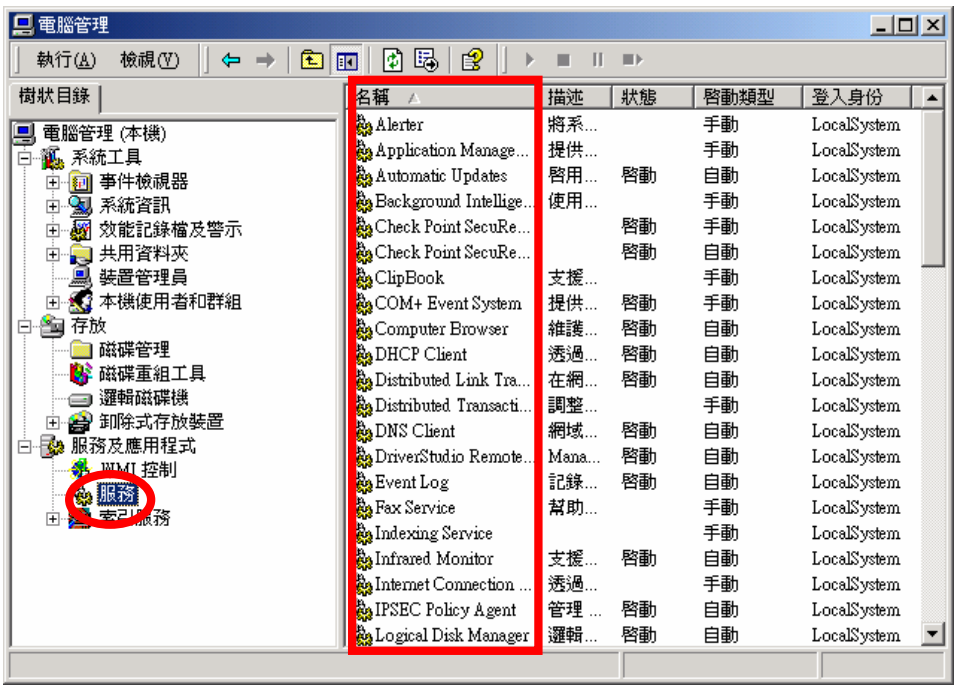
說　　明

檢視系統服務之方法：

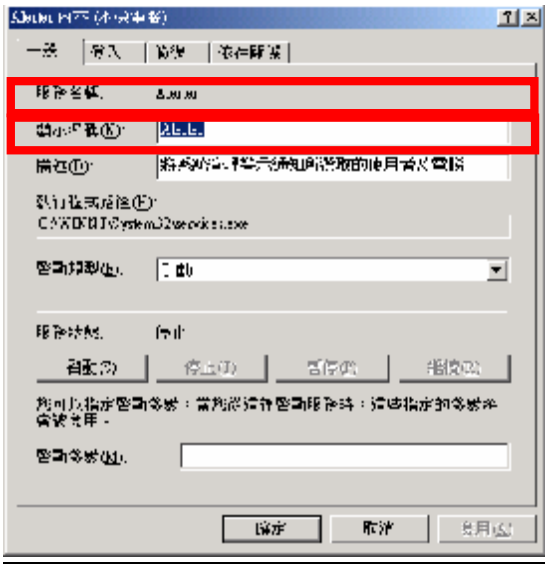
Step1：在「我的電腦」按右鍵，選「管理」。



Step2：點選「服務」。



Step3：檢視服務名稱、顯示名稱及執行程式路徑。



執行步驟

後門名稱：KLGR_MSGina32

說　　明

此為密碼截聽程式

檢　　視

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs 的值。
   * 該值的資料在正常情況下應該為 NULL (無資料)，若不為 NULL，記錄該值內容中之檔案路徑。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL
   * 該機碼在正常情況下應該不存在，若存在，則記錄該值內容中之檔案路徑。

移除方法

1. 設定 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs 的資料為 NULL (清成空白)
2. 刪除 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL
3. 重新開機。
4. 刪除 1、2 中機碼值所指向的檔案 (放在 %systemdir% 下)
5. 刪除 regsvr.exe (放在 %systemdir% 下) PS.不一定會有這個檔案。
6. 更改系統上所有的密碼。

後門名稱：BKDR_RAC.A~D

檢　　視

服務名稱: Saes
顯示名稱: Security Accounts Events

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Saes 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

檢　　視

服務名稱: Seae
顯示名稱: Security Accounts Event

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Seae 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

檢　　視

服務名稱: SAE
顯示名稱: Security Accounts Events

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SAE 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

檢　　視

服務名稱: Netconwork
顯示名稱: Network Connections Workstations

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netconwork 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

檢　　視

服務名稱: Remote Access
顯示名稱: Remote Access

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Remote Access 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

檢　　視

服務名稱: WinMgts
顯示名稱: Windows Management Sessions

移除方法

1. 刪除 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\
   下的值: nethlpsvcs　資料: WinMgts

2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\下的值: DependOnService 資料: WinMgts
3. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinMgts 機碼。
4. 刪除 %windir%\system32\svchost.dll 檔案。
5. 重新開機。

後門名稱：BKDR_RAC.E

檢　　視

服務名稱: DhcpSvrView
顯示名稱: DHCP Client View

移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DhcpSvrView 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

後門名稱：BKDR_UMGR

檢　　視

服務名稱: Multimedia Services
顯示名稱: Multimedia Services

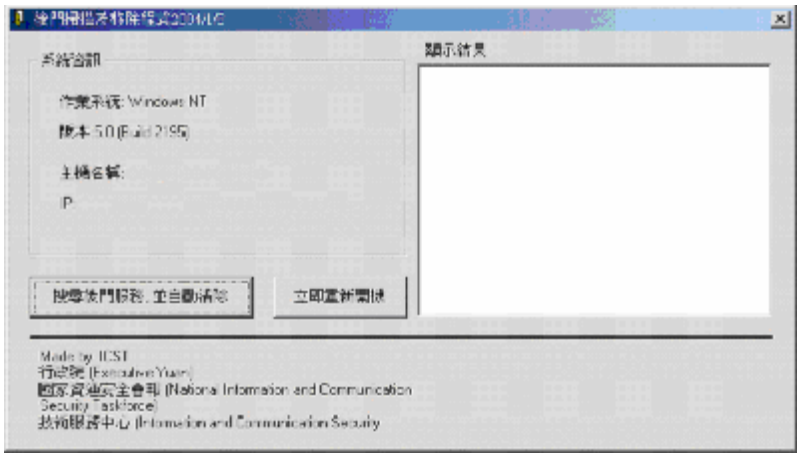
移除方法

1. 點選「服務狀態:」下的「停止」按鈕。
2. 刪除 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Multimedia Services 機碼。
3. 刪除「執行程式路徑」中所指向的程式。
4. 重新開機。

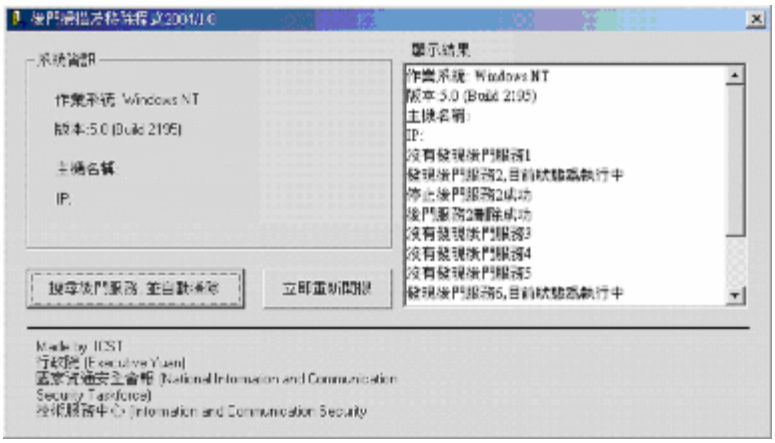
三. 執行後門移除程式

執行步驟

Step1：將 AntiDoor20040108.zip 解壓縮後，執行 AntiDoor20040108.exe
將開啟一個視窗，如以下畫面:



Step2：按下「搜尋後門服務，並自動清除」程式即自動進行搜尋及清除工作，並顯示結果於右方文字框，如以下畫面:



Step3：清除工作完畢，需重新開機。 按下「立即重新開機」重新啟動電腦。

四. 後續處理

1. 檢查主機是否有不正常的帳號。
2. 變更所有帳號之密碼。
3. 檢查主機上是否被安裝/開啟遠端控制程式(r_server、Terminal Service、Dameware Remote Control、VNC、PCAnywhere..)；若無使用，請移除。
   注意：上述服務可能被更名為其他服務名稱，檢視時請特別注意。