香港電腦保安事故協調中心
Hong Kong Computer Emergency Response Team Coordination Centre

移除 「Autorun 病毒」的程序
第 1.1 版

甚麼是「Autorun 病毒」?

「Autorun 病毒」是近期十分流行電腦病毒，這種病毒利用外置儲存裝置的可攜性和視窗系統的自動執行特性來散播。病毒會在受感染的電腦上建立一個執行檔案，並且在所有可以寫入資料的磁碟分區上建立一個隱藏的系統檔案 autorun.inf 和禁止電腦顯示隱藏檔案。若受感染的電腦掛載了可以寫入資料的網絡磁碟或插入外置儲存裝置 (包括 USB 手指、USB 外置硬碟、各種記憶卡、MP3 播放器等)，病毒檔案便會自動複製到這些裝置而受到感染。

注意事項

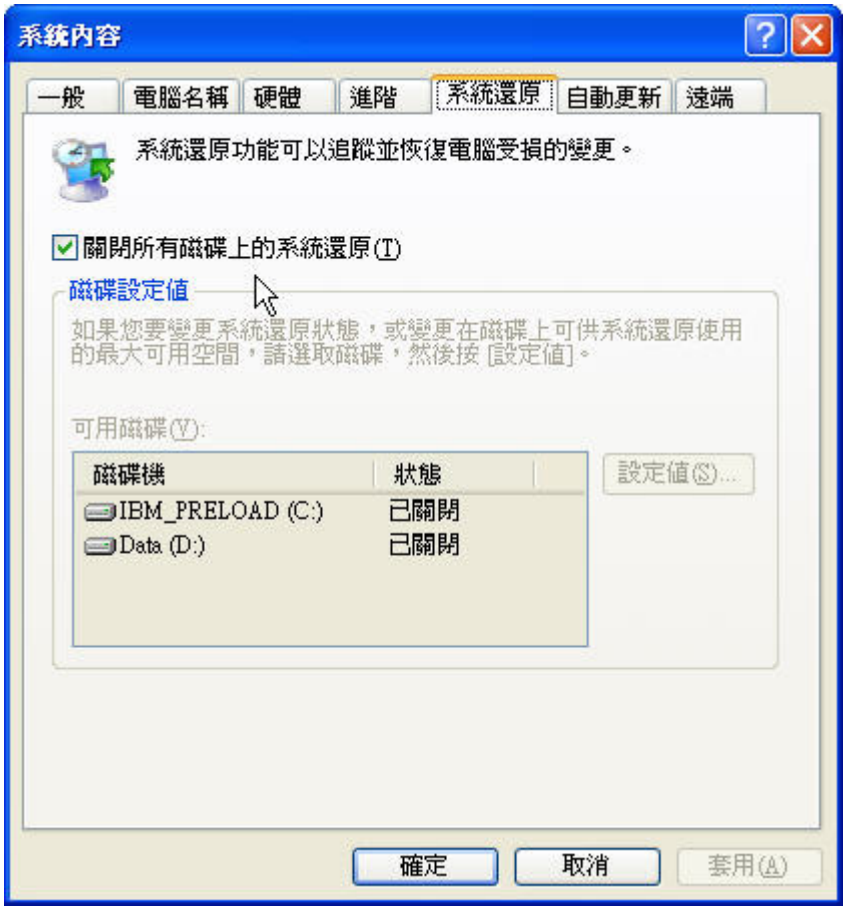
- 這程序是專爲移除「Autorun 病毒」而設，請 **按次序執行所有步驟**。
- 在執行本程序前，建議你先**備份電腦上的數據** (例如把文件、相片、地址簿等，燒錄至 CD-R 或 DVD-R 上) ，以確保系統一旦出現問題時，仍可修復至原來的狀態。
- 本程序提供的數據和資訊祇作參考用途，用戶需要對是否遵循本程序、或移除電腦上的「Autorun 病毒」的決定承擔全部責任。HKCERT 對本程序內容的錯誤、遺漏及用戶因依據提供的資訊所作的任何行爲，而引起的任何損失，概不負責。
- 如果對此程序有任何問題，請聯絡 HKCERT 。
  電話：81056060 電郵： 81059760

由於「Autorun 病毒」暫時沒有可靠的獨立清除程式，需要以 "手動移除方式" 處理。此程序適用於視窗 2000、視窗 XP、視窗 2003、視窗 Vista，請按次序執行以下步驟：

1.將有問題的電腦 (如果超過一部電腦受感染，建議先處理伺服器) 移離網絡，例如：拔走網絡線。否則，病毒可能會擴散到網絡上其他的電腦。

2.關閉系統還原功能 (只適用於視窗 XP 和視窗 Vista)
爲何要關閉系統還原？ - 視窗的系統還原功能會定期(預設是一天)在電腦上建立並儲存「還原點」或偵測到系統上有某些變更，例如：安裝軟件、驅動程式等也會建立「還原點」。「還原點」包含視窗使用的登錄設定和其他系統資訊，但不包括個人檔案 (例如電子郵件、文件或相片)。爲了防止系統仍然將病毒檔案和相關的登錄設定保留在「還原點」內，有可能令我們的清理工作徒勞無功，我們需要關閉系統還原功能來清除「還原點」內的資料。

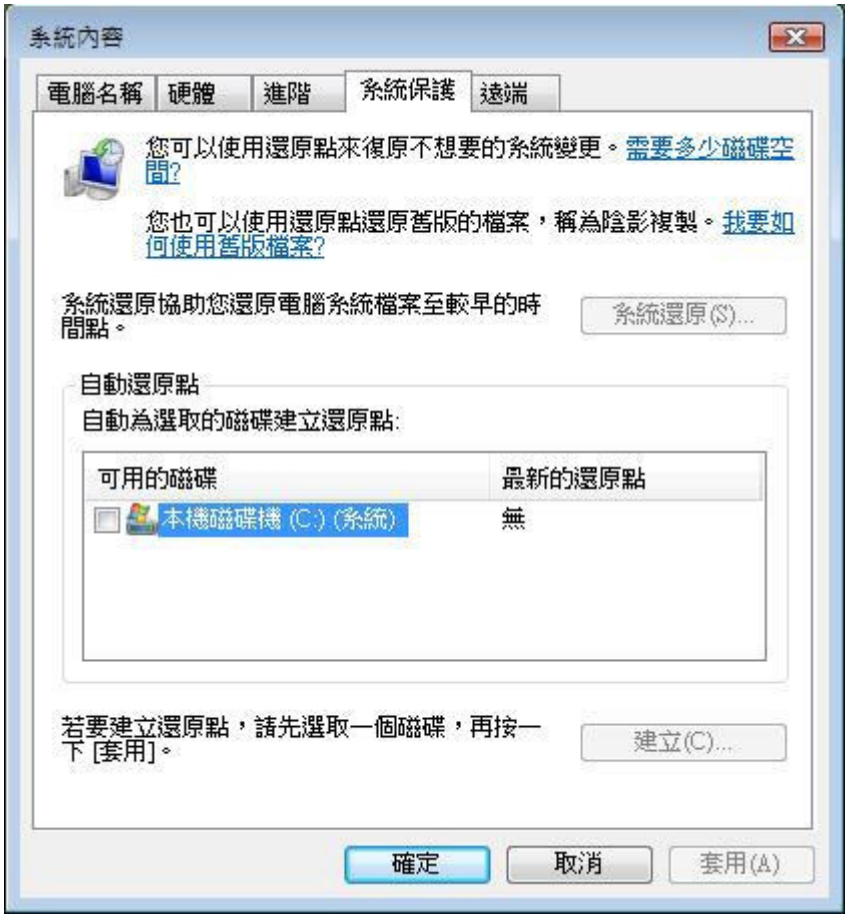
i. 適用於視窗 XP 的步驟
按下「開始」。
在「我的電腦」按下滑鼠右鍵，然後按下「內容」。
按下「系統還原」標籤 [見圖一]。



[圖 一]

勾選「關閉系統還原」或「關閉所有磁碟上的系統還原」然後按下「套用」。
如訊息中所說，這將會刪除所有現存的系統還原，按下「是」。
按下「確定」，重新啓動電腦。

ii. 適用於視窗 Vista 的步驟
按下「開始」。
在「電腦」按下滑鼠右鍵，然後按下「內容」。
按下「系統保護」 [見圖二]。



[圖二]

在「可用的磁碟」，取消勾選屬於系統的本機磁碟機 (預設是 C:)，然後按下「確定」
如訊息中所說，這將會刪除所有現有的還原點，按下「關閉系統還原」。
重新啓動電腦。

3. 移除病毒檔案
i. 開啓檔案總管，記錄現時所有磁碟代號。

ii. 在「開始」->「執行」，輸入 cmd [見圖三]，按「確定」後出現 "命令提示字元"的視窗。

[圖三]

iii. 檢查 autorun.inf 是否存在
輸入 cd \ ，回到 C:\
輸入 attrib autorun.inf
如果發現 autorun.inf 檔案是存在的，輸入 type autorun.inf
你會見到內容大致是這樣的

```
open=[xxx]
shell\open\Command=[xxx]
shell\explore\Command=[xxx]
```

注意： [xxx] 代表病毒檔案名稱，每部受感染的電腦所發現的名稱都可能是不同的，請記錄 [xxx] 檔案名稱

iv. 刪除 autorun.inf 和病毒檔案
輸入 attrib -S -H -R X:\autorun.inf
輸入 attrib -S -H -R X:\[xxx]，如果這個檔案已被刪除或不存在會有找不到檔案的訊息
注意： [X] 代表磁碟代號，所有電腦上連接的儲存媒體 (包括網絡、USB 存儲裝置和各種記憶卡)，[xxx] 代表病毒檔案名稱

輸入 del X:\autorun.inf
輸入 del X:\[xxx]，如果這個檔案已被刪除或不存在會有找不到檔案的訊息
注意： 請小心輸入要刪除的檔案名稱，否則可能錯誤刪除其他檔案

在每一個磁碟代號都要執行上述的步驟，完成後，輸入 exit 離開 "命令提示字元"的視窗。

4. 刪除登錄索引值 (Registry) 內病毒檔案的執行設定

> 注意：以下步驟需要使用"系統登錄編輯程式"來修復視窗登錄索引值 (Windows Registry)，如果你不熟悉視窗登錄索引值的操作，建議你向電腦供應商或朋友尋求協助。不正確更改視窗登錄索引值，有可能令視窗功能運作不正常。

在「開始」->「執行」，在開啓輸入 regedit，按「確定」後出現 "系統登錄編輯程式"視窗。

在 HKCEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

和

在 HKCEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

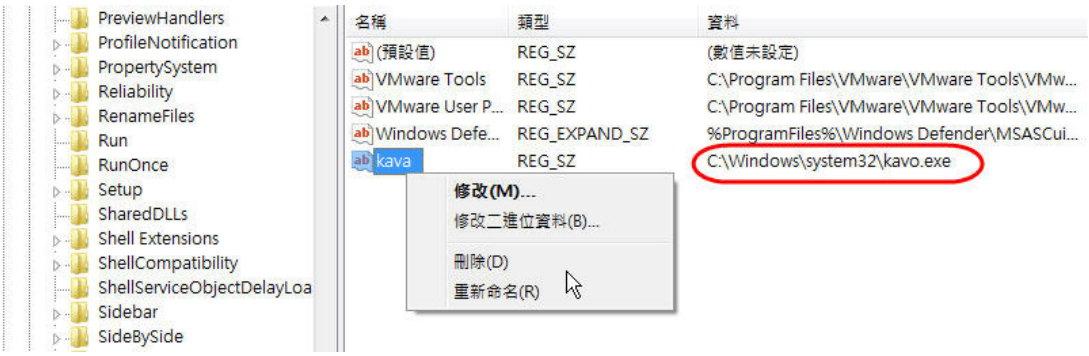
裡找以下的索引值的資料 [見圖四]

i. 視窗 2000 下的索引值

C:\WINNT\System32\[yyy]

ii. 視窗 XP、視窗 2003 和視窗 Vista 下的索引值

C:\WINDOWS\System32\[yyy]



[圖四]

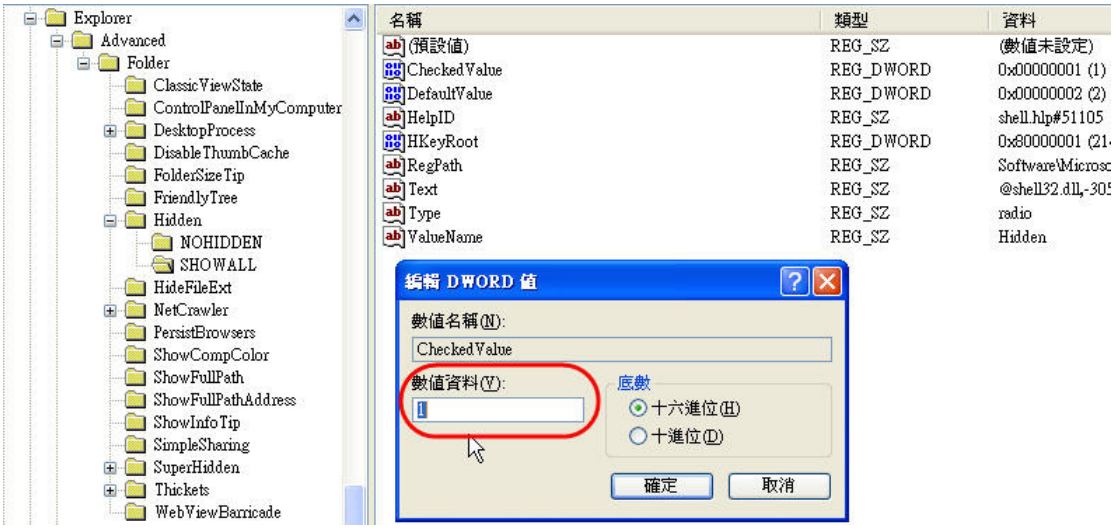
注意：[yyy] 代表病毒檔案名稱，例如：fly.exe, goods.exe, kavo.exe, kavo0~9.dll, mnso.exe, ntdelect.com, ntdelete.com, nx.exe, poor.exe, rxpmon.exe, sos.exe, systom.exe, taso.exe, taso0~9.dll, tavo.exe, ubs.exe, winpows.exe 等 (未能盡錄)，每部受感染電腦所發現的名稱都可能是不同的。如果發現，請記錄 [yyy] 檔案名稱和刪除這個索引值。如果沒有發現，可以依照步驟 7 利用防毒軟件或在線的防毒掃描工具完整掃描系統一次，將病毒檔案移除。

5.解決無法顯示隱藏檔案的問題

在

HKCEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL [見圖五]

裡找 CheckedValue 索引值，開啓它並將數值資料改成 1



[圖五]

6. 如果步驟 (3 - 5) 無法刪除病毒檔案，請重新開機並且連續按 F8，選擇以"安全模式" 進入視窗系統，開啓檔案總管，再次手動刪除之前記錄的 [xxx] 和 [yyy] 病毒檔案。

注意： 請小心檢查檔案名稱，然後才執行刪除。

7. 掃描全系統，尋找未知的病毒檔案

在步驟 3，我們已使用手動刪除方法將一些已知的病毒檔案刪除，但 「Autorun 病毒」的變種日漸增加，我們建議執行一次全系統的病毒掃描，確保一些未知的病毒檔案也可被偵測出來。

a. 如果你有安裝防毒軟件，而且可以連接互聯網，請下載最新病毒定義資料檔案。 如果你的電腦無法連接互聯網，你需要在另一部沒有問題的電腦上下載你們所使用的防毒軟件的最新病毒定義資料檔案，將它燒錄到光碟。之後，啓動有問題的電腦，進入視窗後，插入之前燒錄的光碟，嘗試雙按光碟上的檔案來安裝最新病毒定義資料。成功安裝後，請執行一次全系統掃描。完成後，掃描結果會列出是否有病毒感染和建議的處理方法，依照指示將找到的病毒檔案移除。

b. 如果你沒有安裝防毒軟件，我們建議你使用在線的防毒掃描工具，例如：Windows Live OneCare [見圖六]

[圖六]

步驟如下：

i. 連線到 http://safety.live.com，在 Windows Live OneCare 安全掃描視窗選擇"防護"。在防護中心，按"防護掃描"。

ii. 有一個"服務合約"視窗會顯示介紹使用上的規條，按 "接受" 同意使用。

iii. 在安裝掃描工具，按"立即安裝"，資訊列提示視窗可能會出現，你會見到網址列下會有一個安裝 ActiveX 指示，按一下並選擇安裝 ActiveX 控制項。然後"Internet Explorer 安全性警告視窗" 會出現，問你是否安裝"Windows Live Safety Center Component"，選"安裝"。

iv. 按"啓動掃描工具"，會有一個"防護掃描"視窗，選"下一步"便會開始下載掃描工具，需時 5-15 分鐘 ，視乎連線的速度。

v. 下載完成後，自行開始掃描電腦上的所有儲存裝置。檢查時間視乎硬碟大小、檔案多少等，一般要 1-2 小時。

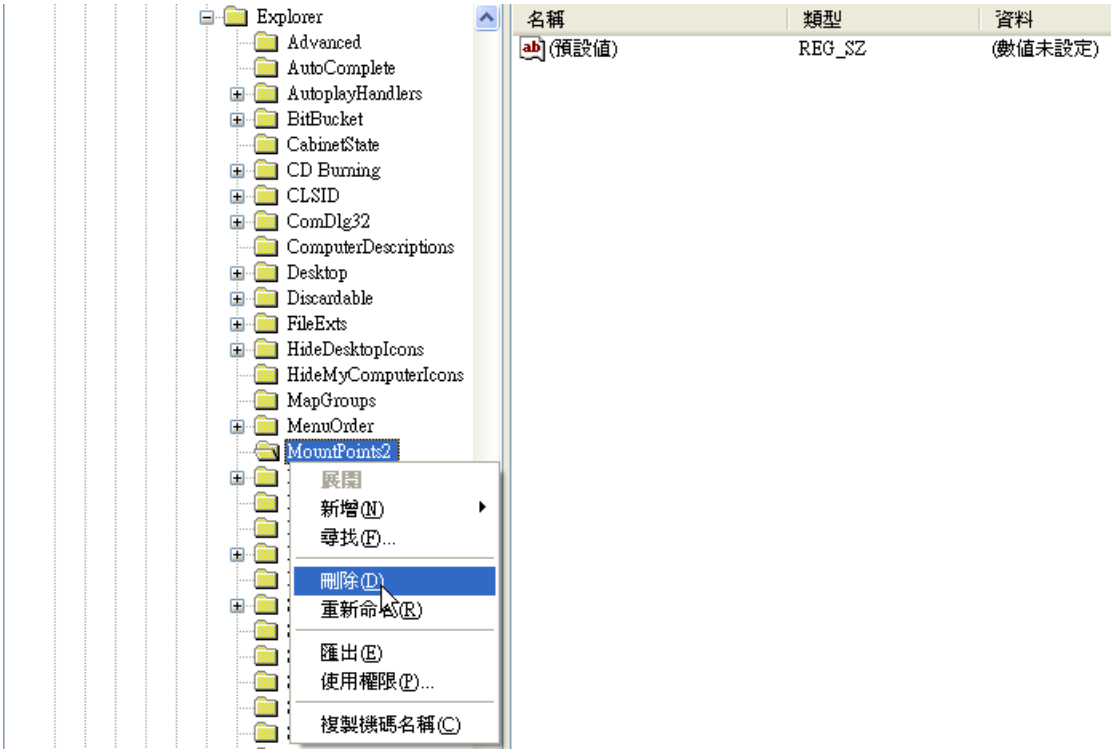
vi. 完成後，掃描結果會列出是否有病毒感染和建議的處理方法，依照指示將找到的病毒檔案移除。

8. 刪除 MountPoints2 登錄機碼 **[更新於 2009 年 1 月 22 日]**

視窗系統可能會在 MountPoints2 登錄機碼記錄之前那些連接過該電腦的裝置內 AutoRun 資料，即使你關閉了自動執行功能，當那些舊有裝置連接到你的電腦後仍然會執行 Autorun 內的指令。基於這個原因，我們建議你在曾經受感染的電腦上刪除以下的 MountPoints2 登錄機碼：

i. 在「開始」->「執行」，在開啓輸入 regedit，按「確定」後出現 "系統登錄編輯程式"視窗。

ii. 在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 [見圖七]



[圖七]

iii. 在 “MountPoints2” 按下滑鼠右鍵，然後按下 ”刪除” 。

iv. 有一個確認信息匣“你確認要刪除這個機碼及其所有子機碼?” 出現，然後按下「確定」。

v. 重新開機讓系統重設 MountPoints2 登錄機碼。

9. 恢復系統還原功能 (還原步驟 2，只適用於視窗 XP 和視窗 Vista)

I. 適用於視窗 XP 的步驟

i. 按下「開始」。

ii. 在「我的電腦」按下滑鼠右鍵，然後按下「內容」。

iii. 按下「系統還原」標籤。

iv. 取消勾選「關閉系統還原」或「關閉所有磁碟上的系統還原」。

v. 按下「套用」，然後按下「確定」。

vi. 重新啓動電腦。

II. 適用於視窗 Vista 的步驟

i. 按下「開始」。

ii. 在「我的電腦」按下滑鼠右鍵，然後按下「內容」。

iii. 按下「系統保護」。

iv. 在「可用的磁碟」，勾選屬於系統的本機磁碟機 (預設是 C:)。

v. 按下「套用」，然後按下「確定」。

vi. 重新啓動電腦。

- 完 -