這隻隨身碟病毒不會破壞檔案，請安心慢慢繼續看下去該如何應對...

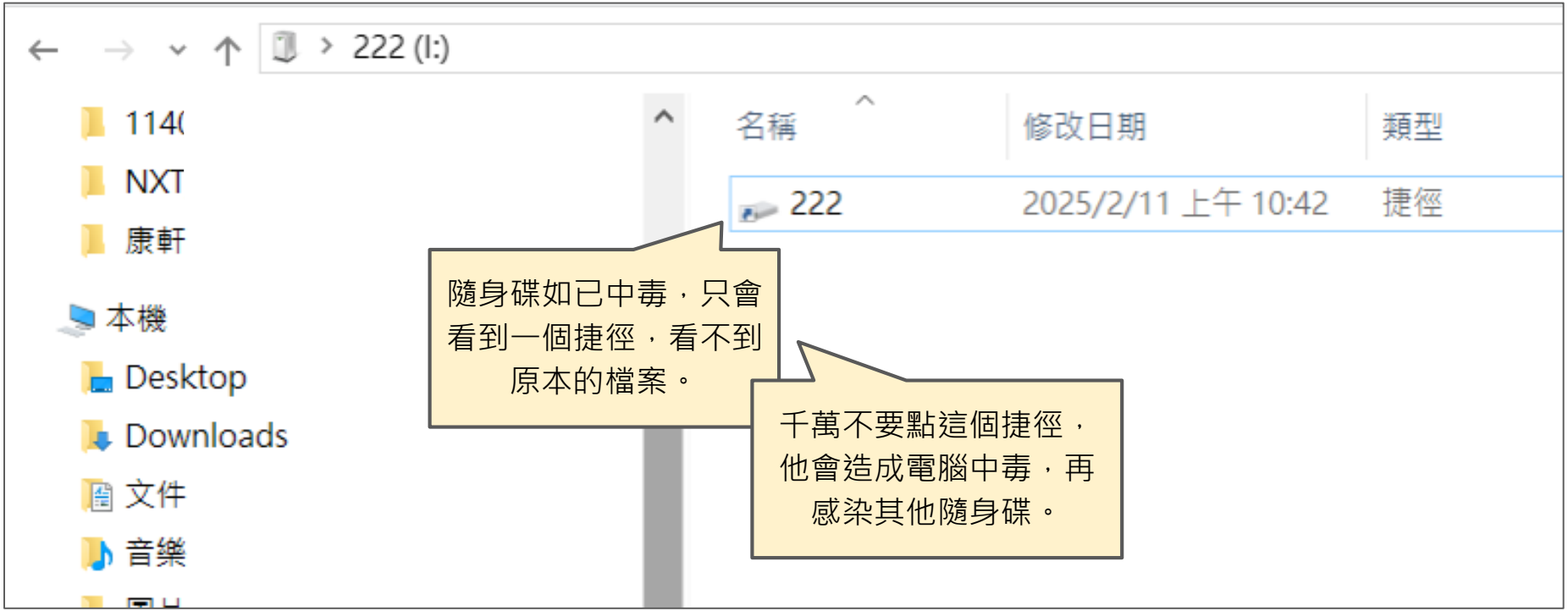
內容大綱：

1. 隨身碟已中毒，如何開啟檔案
2. 如何清理隨身碟病毒
3. 如何檢查電腦是否中毒
4. 本次隨身碟病毒概述
5. 如何清除這隻電腦病毒

1. 隨身碟已中毒

如何開啟存在其中的檔案

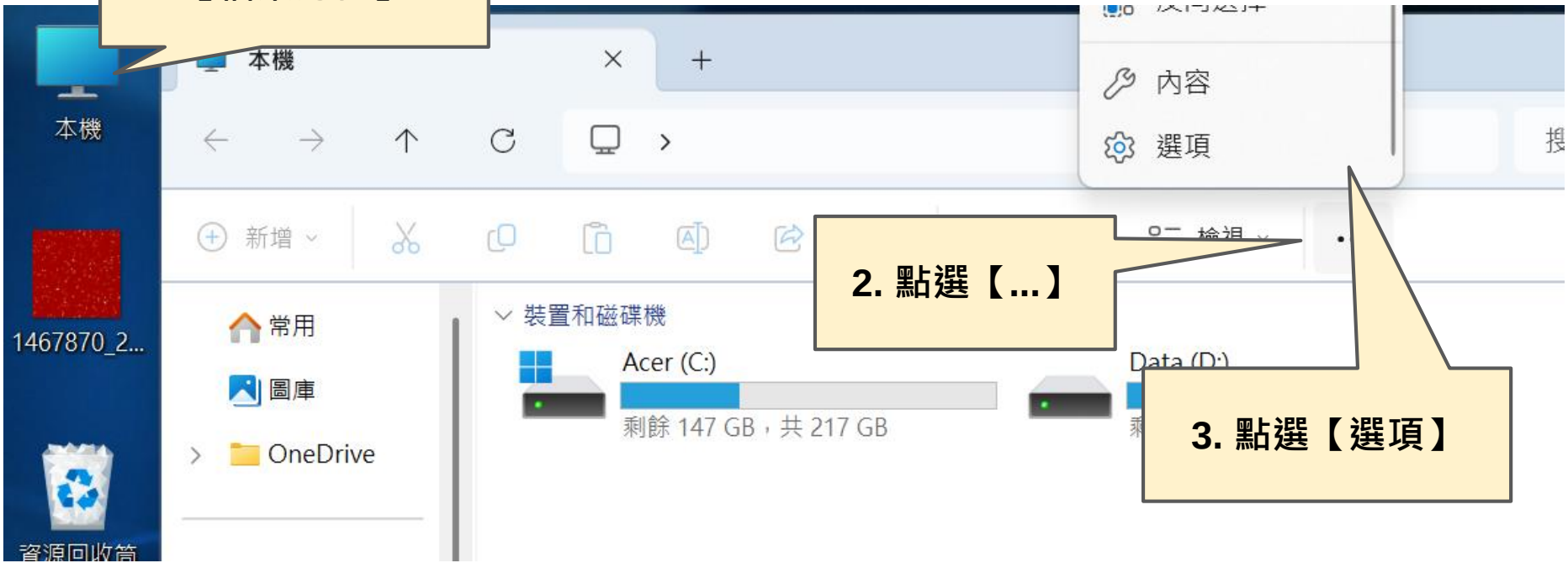
首先，千萬不要點開捷徑，會造成電腦中毒

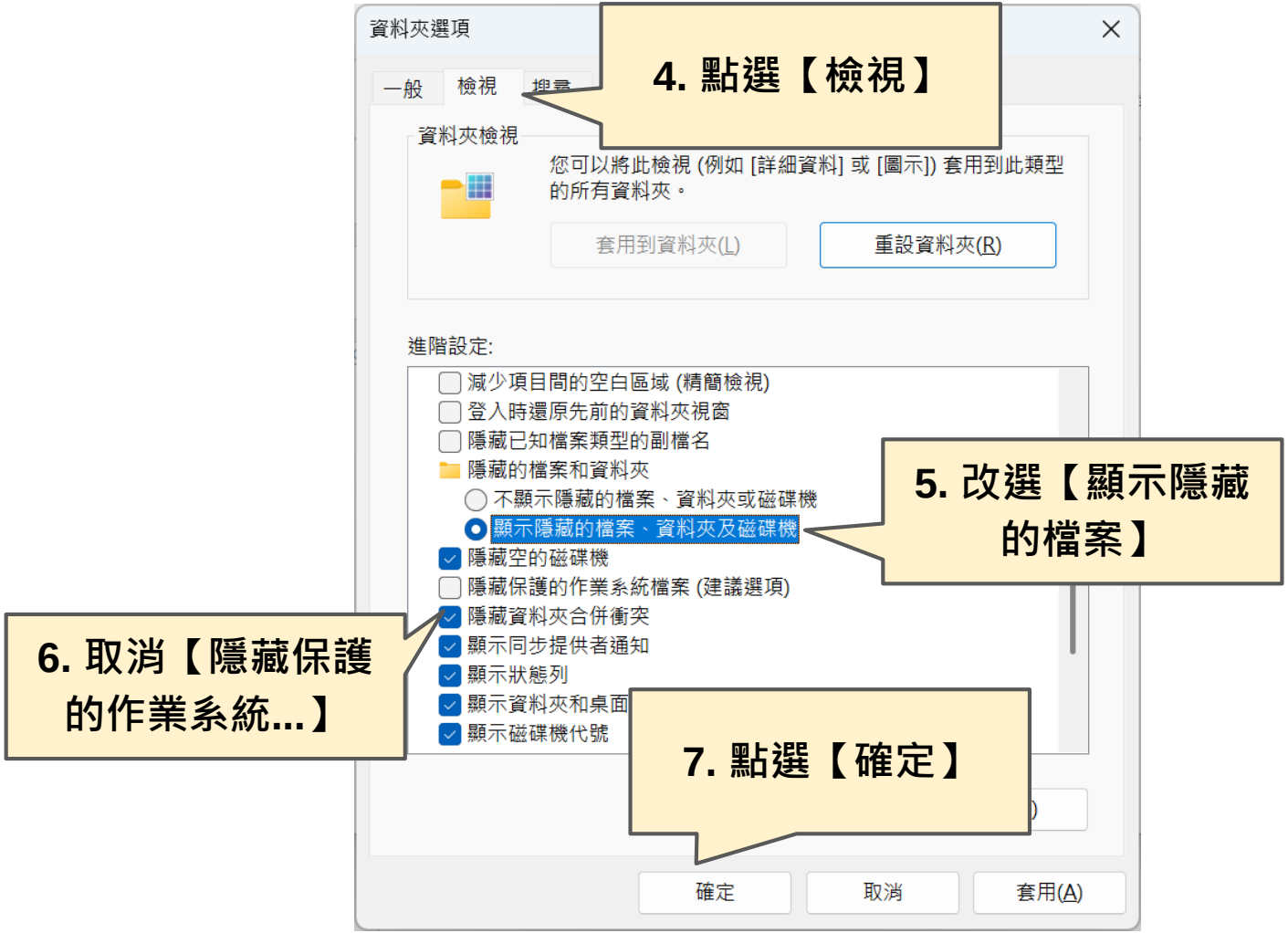


2. 如何清理隨身碟裡的病毒

如果覺得以下步驟很複雜，請找身邊電腦高手或來找我都可以

準備工作：讓病毒檔案現形

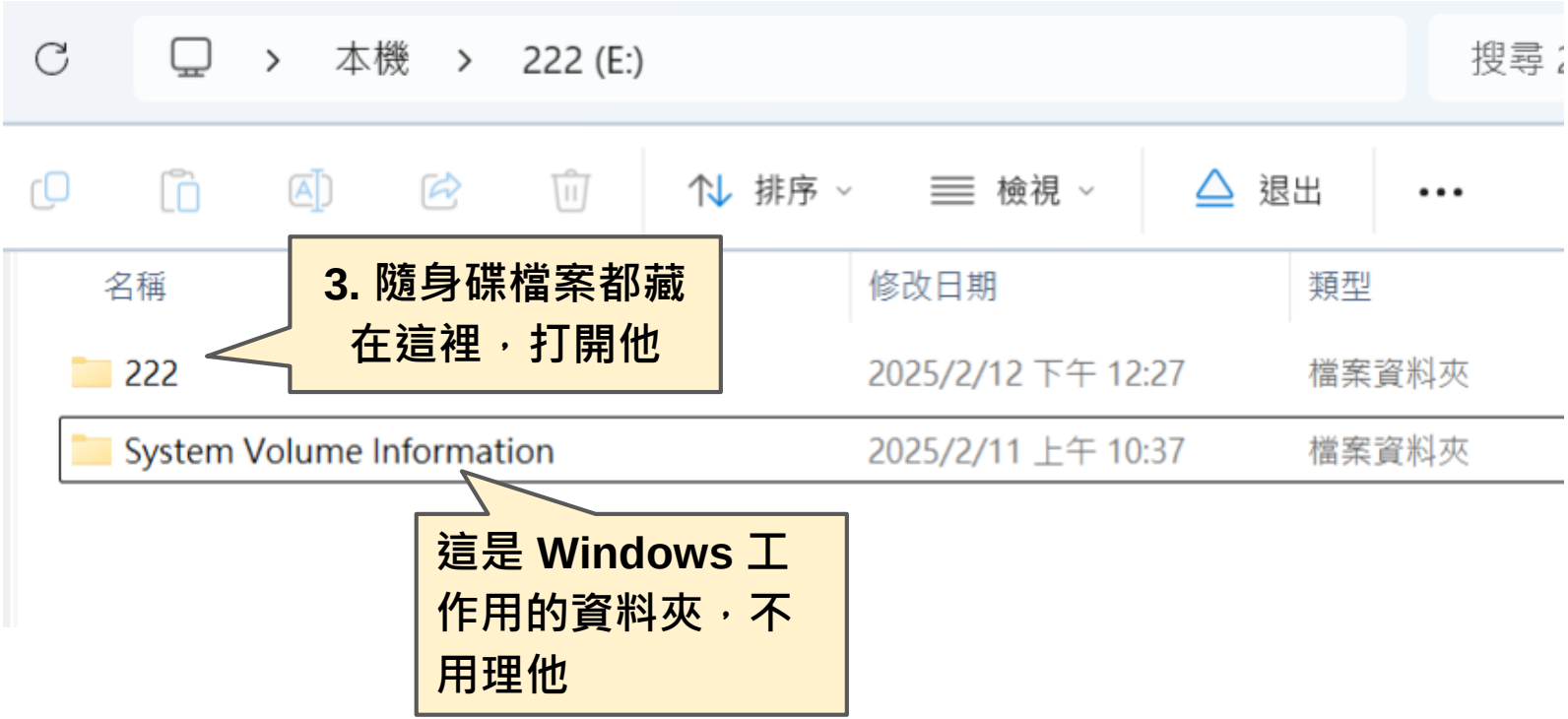


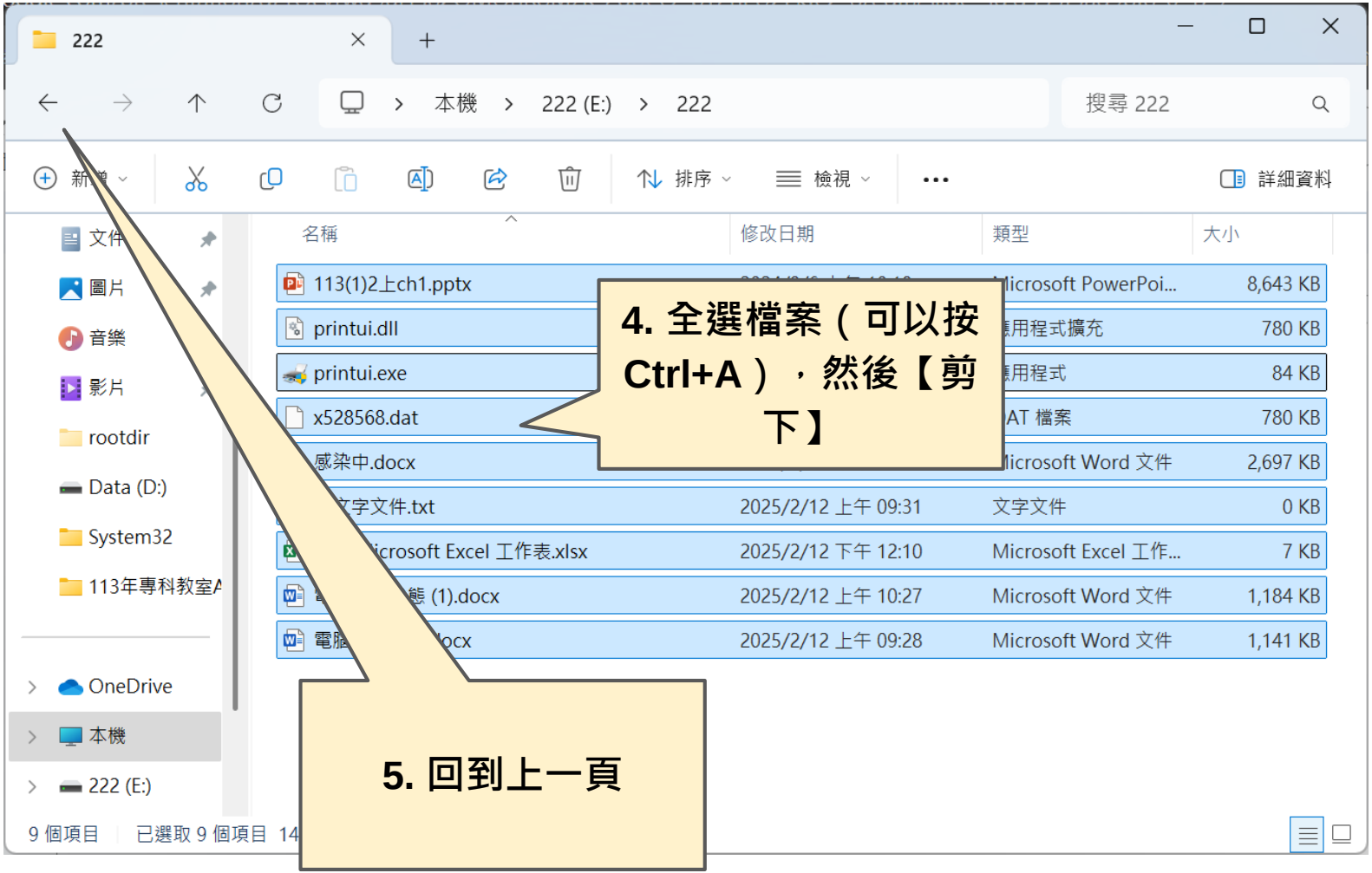

資料夾選項
一般
檢視
搜尋
4. 點選【檢視】
資料夾檢視
您可以將此檢視 (例如 [詳細資料] 或 [圖示]) 套用到此類型的所有資料夾。
套用到資料夾(L)
重設資料夾(R)
進階設定:
減少項目間的空白區域 (精簡檢視)
登入時還原先前的資料夾視窗
隱藏已知檔案類型的副檔名
隱藏的檔案和資料夾
不顯示隱藏的檔案、資料夾或磁碟機
顯示隱藏的檔案、資料夾及磁碟機
隱藏空的磁碟機
隱藏保護的作業系統檔案 (建議選項)
隱藏資料夾合併衝突
顯示同步提供者通知
顯示狀態列
顯示資料夾和桌面
顯示磁碟機代號
5. 改選【顯示隱藏的檔案】
6. 取消【隱藏保護的作業系統...】
7. 點選【確定】
確定
取消
套用(A)

開啟中毒的隨身碟


本機
222 (E:)
搜尋
排序
檢視
退出
名稱
修改日期
類型
222
2025/2/12 下午 12:27
檔案資料夾
rootdir
2025/2/11 下午 04:10
檔案資料夾
System Vo
2025/2/11 上午 10:37
檔案資料夾
222
2025/2/12 上午 09:29
捷徑
1. 這是存放病毒的資料夾，刪除
2. 這是病毒產生的騙人捷徑，刪除

到這裡應該只剩兩個資料夾

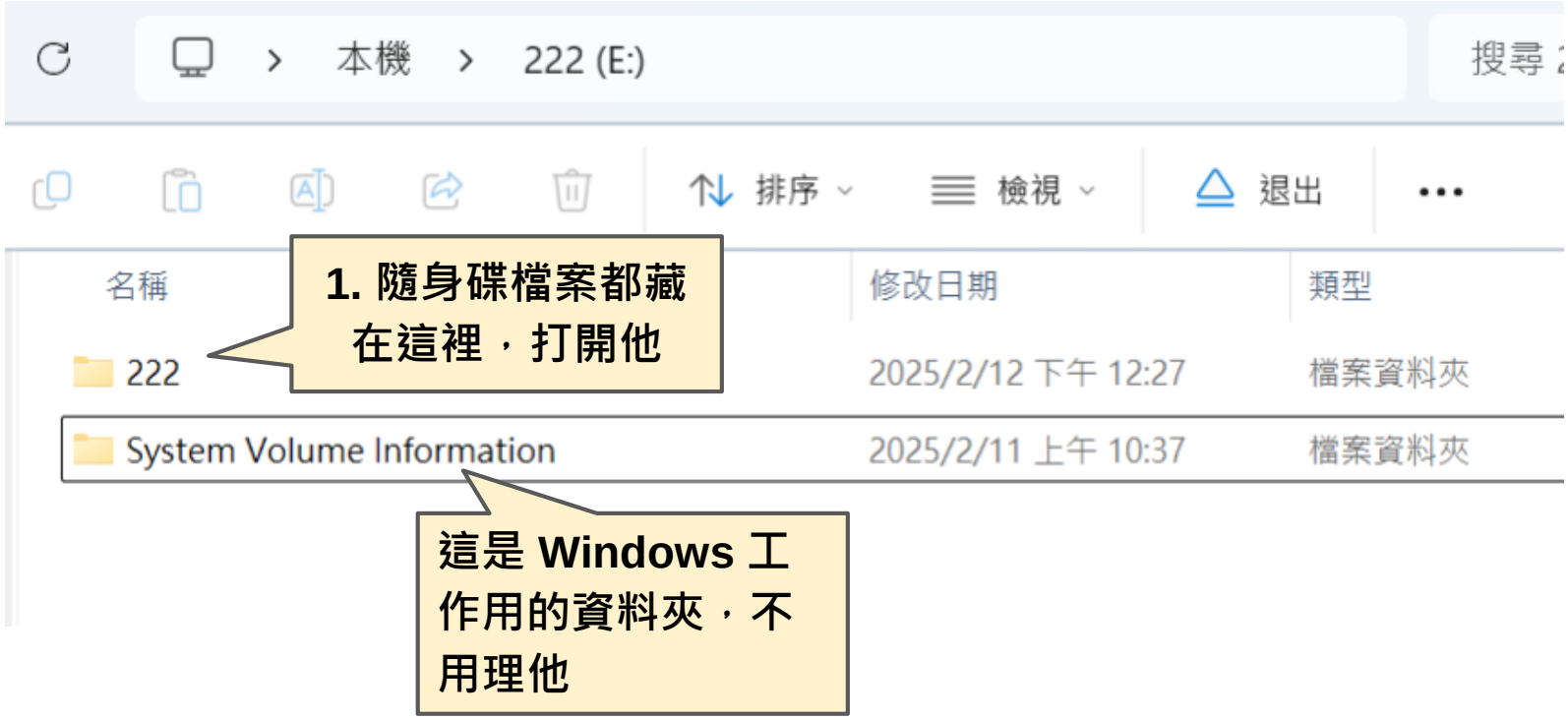



222
本機 › 222 (E:) › 222
搜尋 222
新增
排序
檢視
詳細資料
文件
圖片
音樂
影片
rootdir
Data (D:)
System32
113年專科教室A
OneDrive
本機
222 (E:)
名稱
修改日期
類型
大小
113(1)2上ch1.pptx
Microsoft PowerPoi...
8,643 KB
printui.dll
應用程式擴充
780 KB
printui.exe
應用程式
84 KB
x528568.dat
DAT 檔案
780 KB
感染中.docx
Microsoft Word 文件
2,697 KB
文字文件.txt
2025/2/12 上午 09:31
文字文件
0 KB
Microsoft Excel 工作表.xlsx
2025/2/12 下午 12:10
Microsoft Excel 工作...
7 KB
態 (1).docx
2025/2/12 上午 10:27
Microsoft Word 文件
1,184 KB
電腦
2025/2/12 上午 09:28
Microsoft Word 文件
1,141 KB
9 個項目
已選取 9 個項目
4. 全選檔案（可以按 Ctrl+A），然後【剪下】
5. 回到上一頁


222 (E:)
本機 > 222 (E:)
搜尋 222 (E:)
新增
排序
檢視
詳細資料
文件
圖片
音樂
影片
rootdir
Data (D:)
System32
113年專科教室A
OneDrive
本機
名稱
修改日期
類型
大小
222
2025/2/12 下午 01:53
檔案資料夾
System Volume Information
2025/2/11 上午 10:37
檔案資料夾
113(1)2上ch1.pptx
8,643 KB
printui.dll
780 KB
printui.exe
84 KB
x528568.dat
780 KB
感染中.docx
2,697 KB
新文字文件.txt
2025/2/12 上午 09:31
0 KB
新增 Microsoft Excel 工作表.xlsx
7 KB
電腦正常狀態 (1).docx
1,184 KB
電腦正常狀態.docx
2025/2/12
1,141 KB
6. 貼上
檔案就移動過來了
7. 這個資料夾沒用了，
可以刪除了

賀！清毒成功！

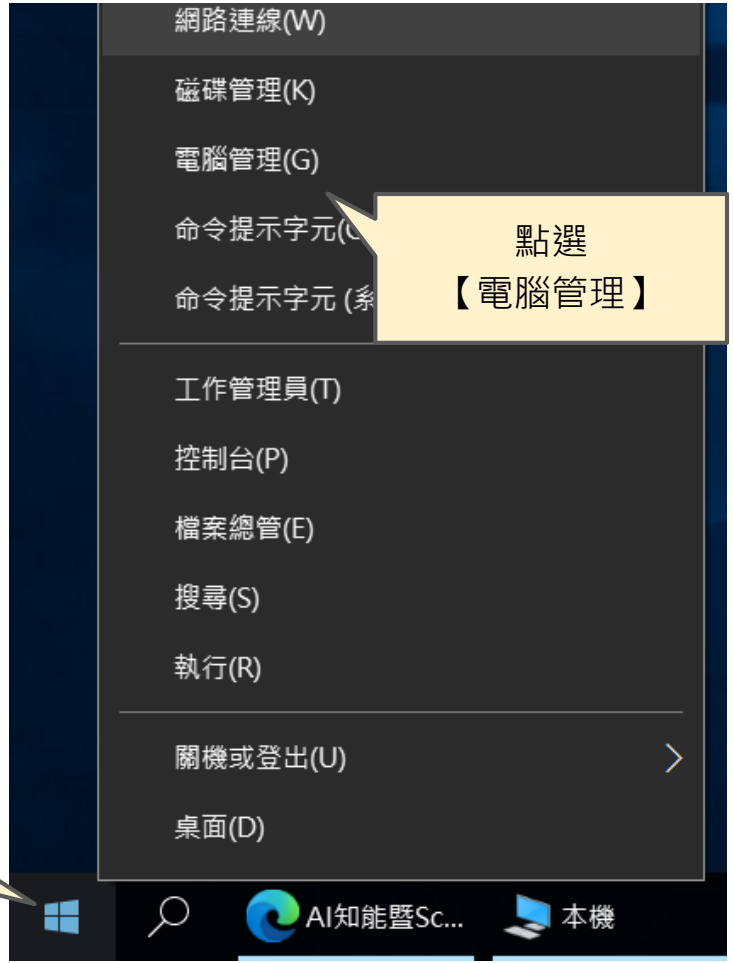
到這裡應該只剩兩個資料夾



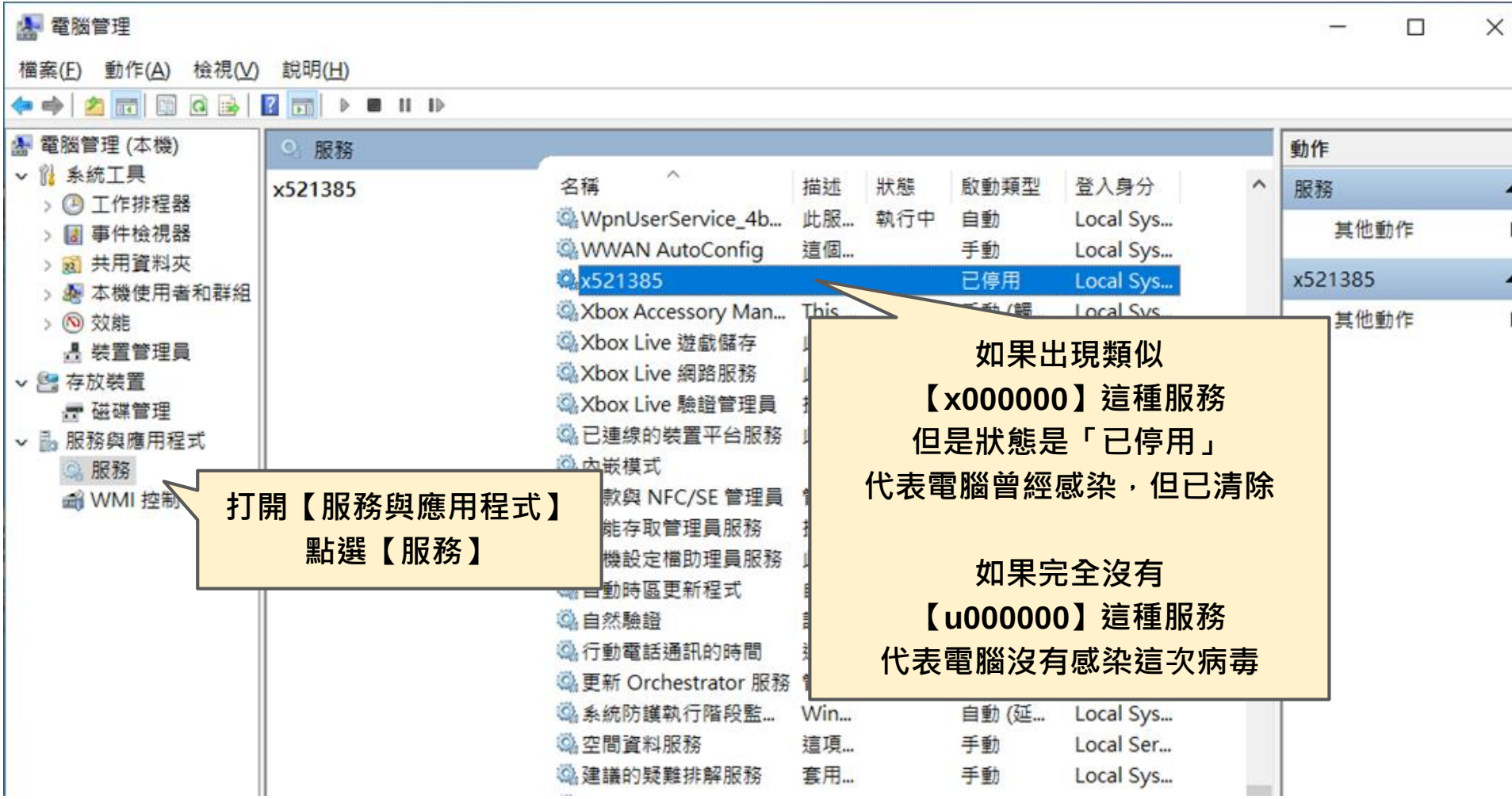
3. 檢查電腦是否中毒

如果插上隨身碟，隨身碟的檔案瞬間消失只剩下一個捷徑，那麼電腦就是病毒且在發作狀態。

在沒有連接隨身碟的狀態下，可參考右圖說明檢查是否有病毒。



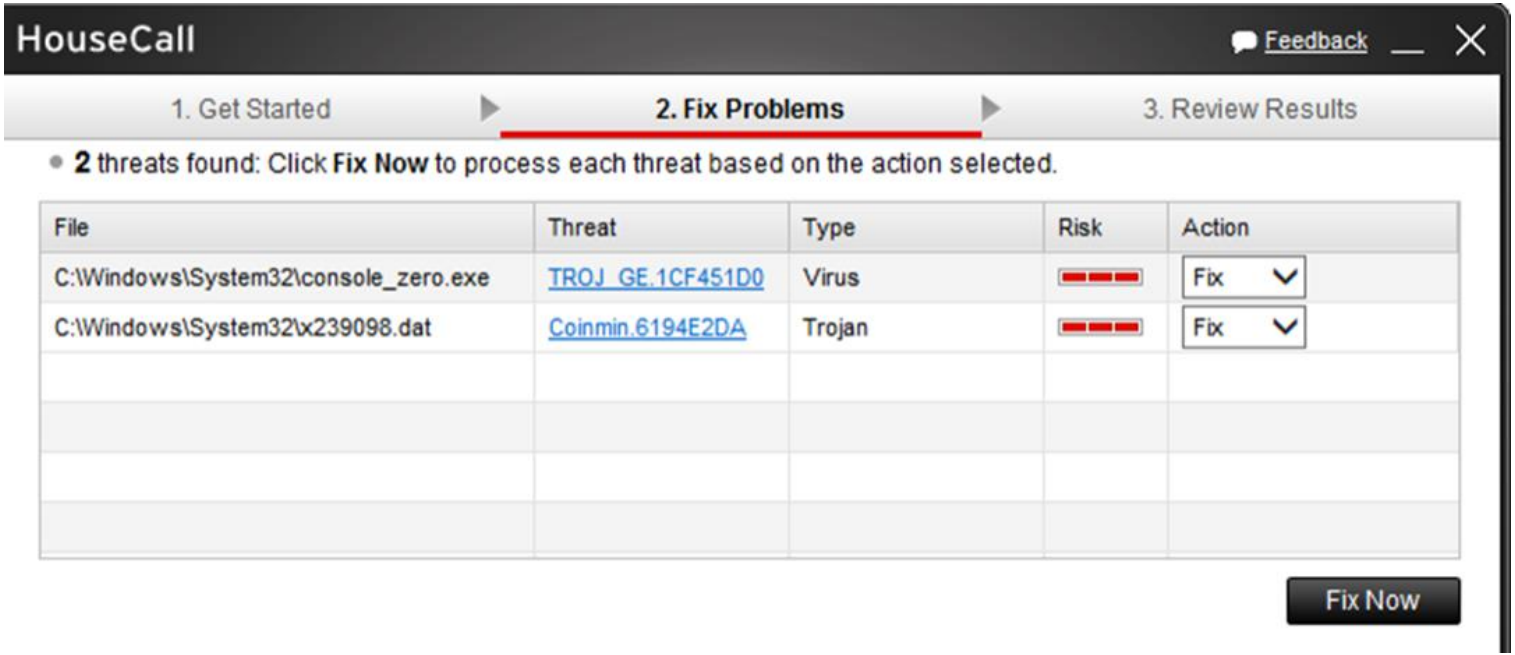

電腦管理 (本機)
系統工具
工作排程器
事件檢視器
共用資料夾
本機使用者和群組
效能
裝置管理員
存放裝置
磁碟管理
服務與應用程式
服務
WMI
打開【服務與應用程式】
點選【服務】
服務
x450853
停止服務
重新啟動服務
名稱
描述
狀態
啟動類型
登入身分
Windows 測試人員服務 提供 ... 手動 (觸... Local Sys...
Windows 感知服務 使空... 手動 (觸... Local Ser...
Windows 感知模擬服務 提供... 手動 Local Sys...
Windows 管理服務 執行... 手動 Local Sys...
WinHTTP Web Proxy Auto-... Win...
Wired AutoConfig 有線...
WLAN AutoConfig WLA...
WMI Performance Adapter 提供...
Work Folders 此服...
Workstation 建立...
WpnUserService_79af1 此服...
WWAN AutoConfig 這個... 手動 Local Sys...
x450853 執行中 自動 Local Sys...
Xbox Accessory Managem... This ... 手動 (觸... Local Sys...
Xbox Live 遊戲儲存 此服... 手動 (觸... Local Sys...
Xbox Live 網路服務 此服... 手動 Local Sys...
如果出現類似
【u000000】這種服務
而且狀態是「執行中」
電腦就是感染病毒了


電腦管理
檔案(F) 動作(A) 檢視(V) 說明(H)
電腦管理 (本機)
系統工具
工作排程器
事件檢視器
共用資料夾
本機使用者和群組
效能
裝置管理員
存放裝置
磁碟管理
服務與應用程式
服務
WMI 控制
服務
x521385
名稱 描述 狀態 啟動類型 登入身分
WpnUserService_4b... 此服... 執行中 自動 Local Sys...
WWAN AutoConfig 這個... 手動 Local Sys...
x521385 已停用 Local Sys...
Xbox Accessory Man... This... Local Sys...
Xbox Live 遊戲儲存
Xbox Live 網路服務
Xbox Live 驗證管理員
已連線的裝置平台服務
內嵌模式
款與 NFC/SE 管理員
能存取管理員服務
機設定檔助理員服務
自動時區更新程式
自然驗證
行動電話通訊的時間
更新 Orchestrator 服務
系統防護執行階段監... Win... 自動 (延... Local Sys...
空間資料服務 這項... 手動 Local Ser...
建議的疑難排解服務 套用... 手動 Local Sys...
動作
服務
其他動作
x521385
其他動作
打開【服務與應用程式】
點選【服務】
如果出現類似
【x000000】這種服務
但是狀態是「已停用」
代表電腦曾經感染，但已清除
如果完全沒有
【u000000】這種服務
代表電腦沒有感染這次病毒

4. 這隻病毒目的為何？

隨身碟檔案被隱藏，並未受到破壞，留下誘餌捷徑藉以欺騙使用者繼續點選執行，達到大量感染電腦。

透過【趨勢科技housecall】掃毒服務，可以抓到兩個病毒檔案，研判此為網路挖礦(coin mining)病毒



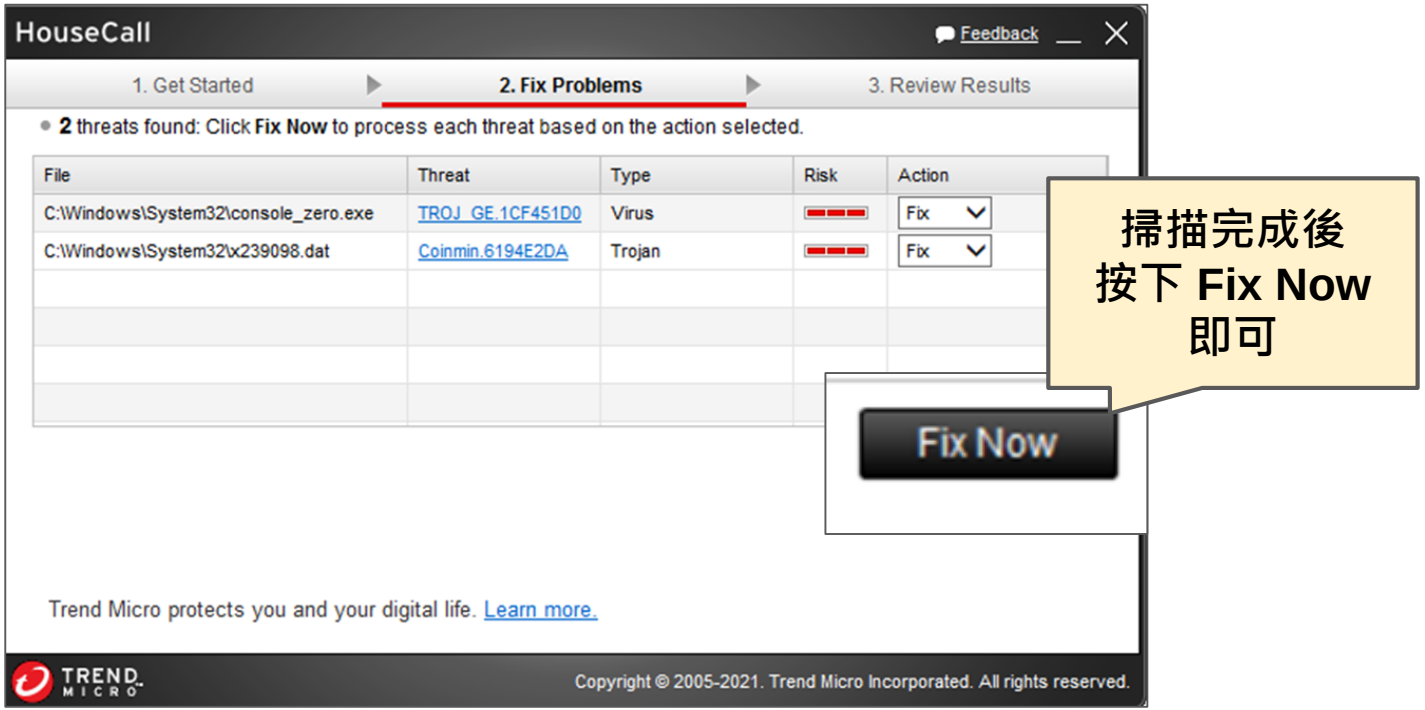
5. 如何清除電腦病毒？

5-1 透過掃毒軟體清毒

5-2 手動清毒（只需三步驟）

5-1.使用【趨勢科技housecall】

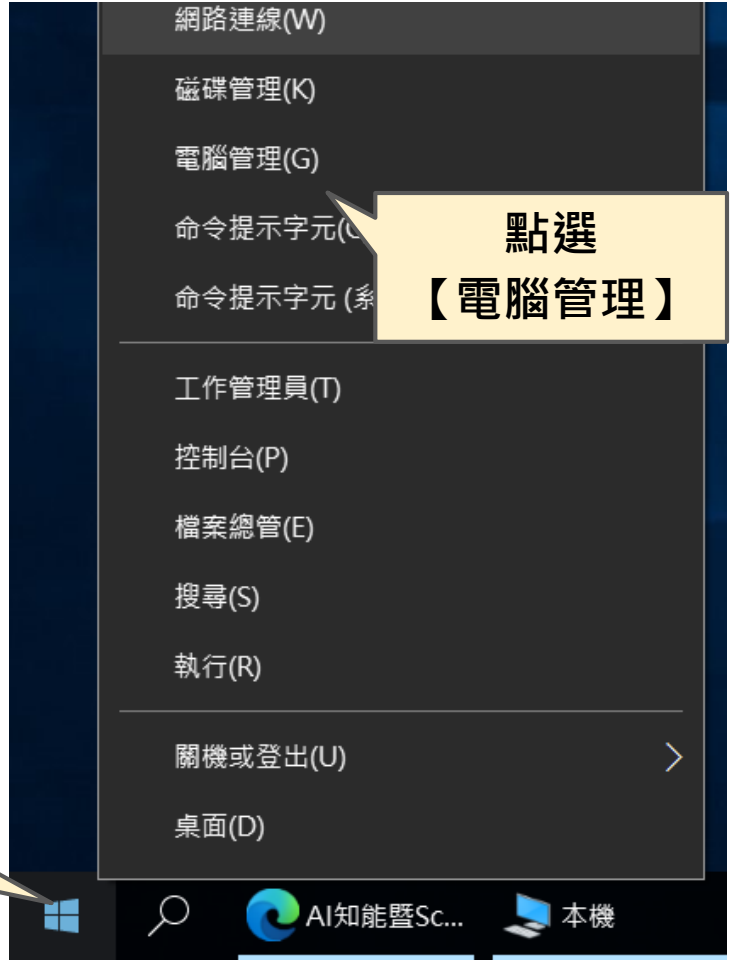
https://www.trendmicro.com/zh_hk/forHome/products/housecall.html

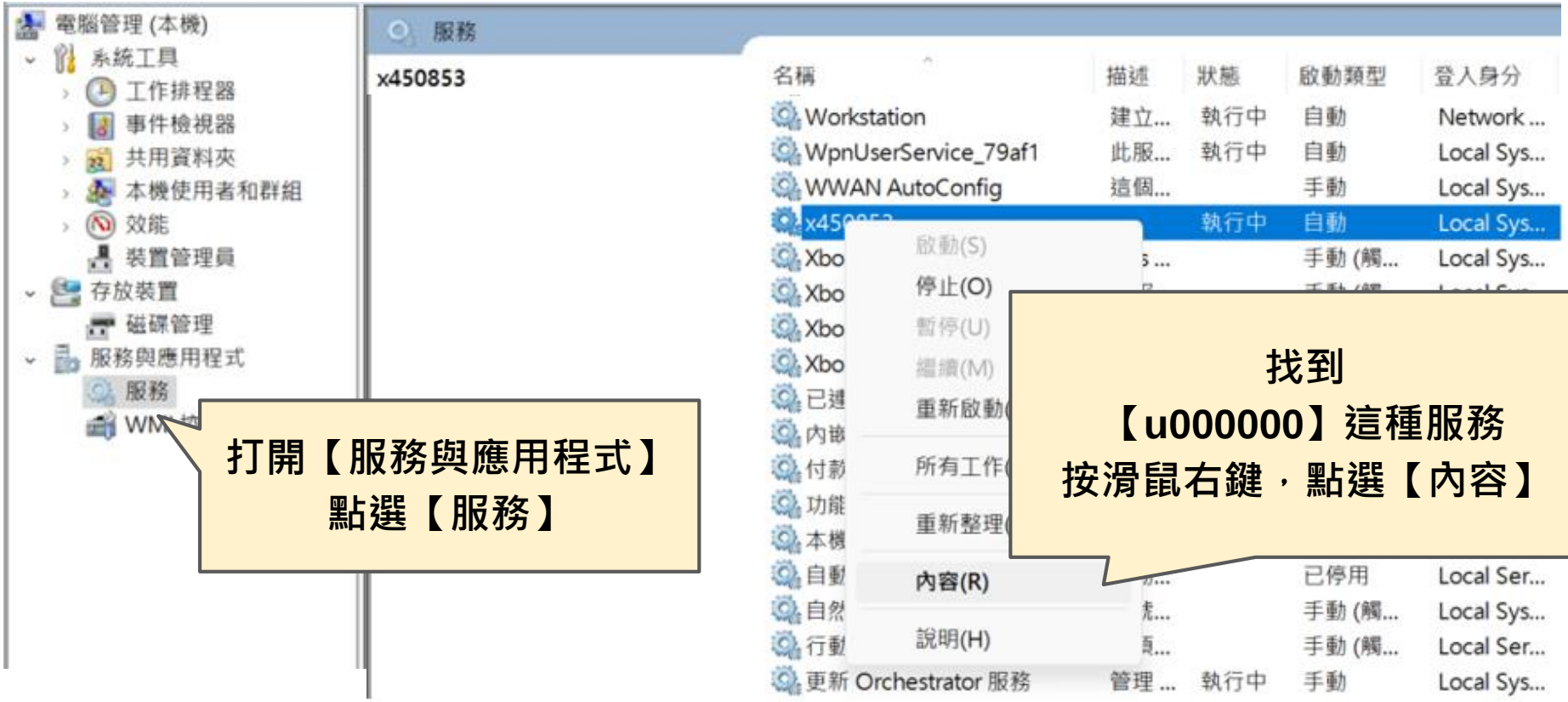


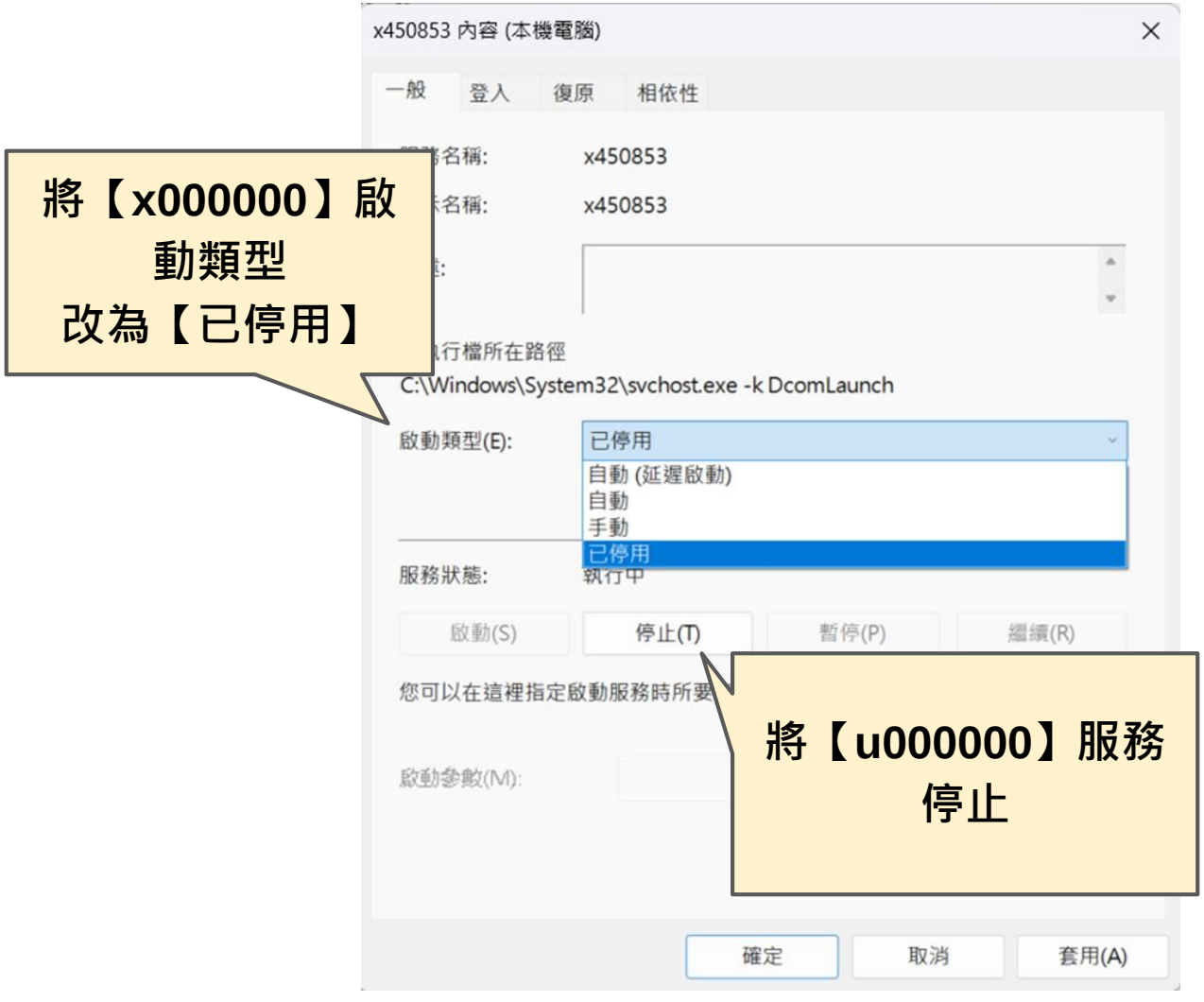
5-2. 手動刪除病毒

若不想等掃毒軟體掃描整台電腦，可手動刪除病毒

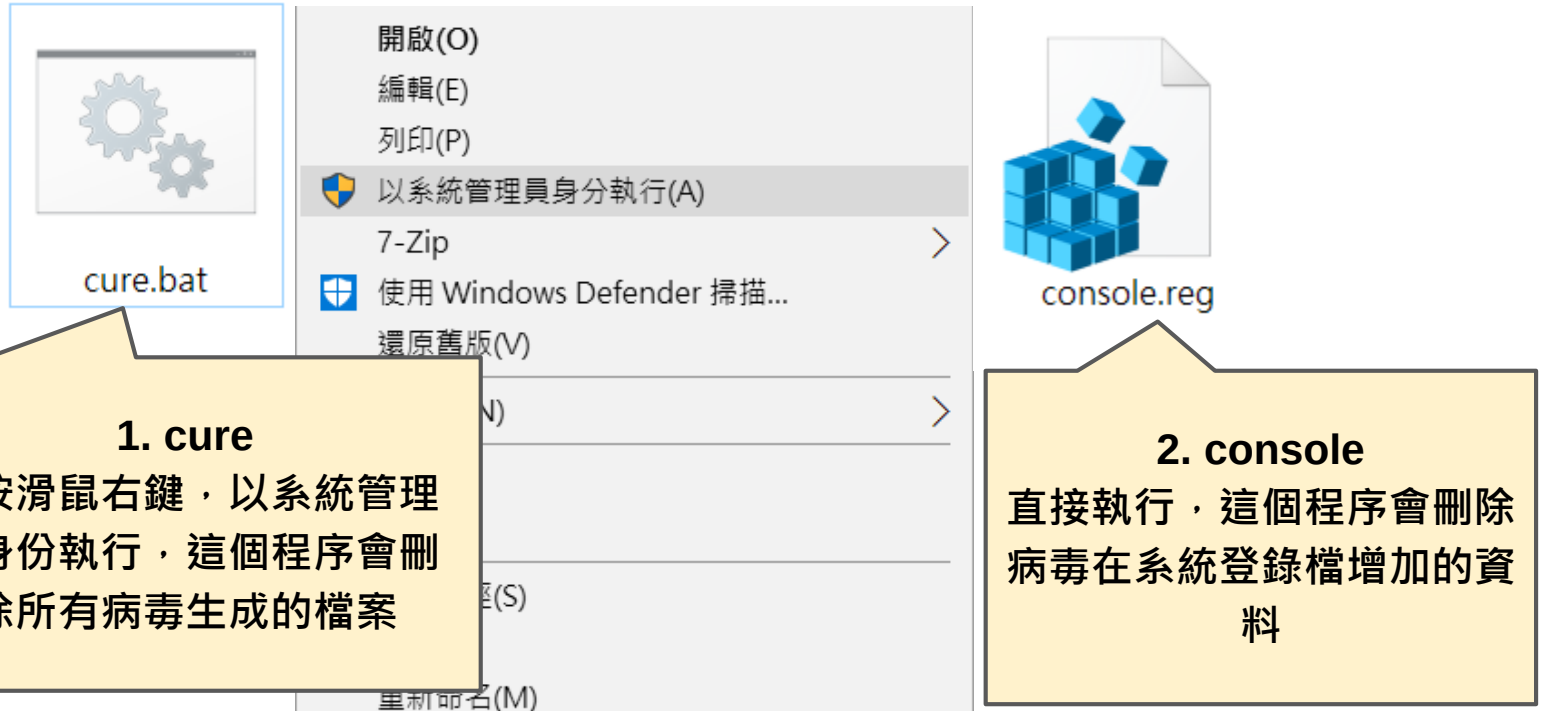
- 停止病毒程序
- 執行 cure
- 執行 console




電腦管理 (本機)
系統工具
工作排程器
事件檢視器
共用資料夾
本機使用者和群組
效能
裝置管理員
存放裝置
磁碟管理
服務與應用程式
服務
服務
x450853
名稱
描述
狀態
啟動類型
登入身分
Workstation
建立...
執行中
自動
Network ...
WpnUserService_79af1
此服...
執行中
自動
Local Sys...
WWAN AutoConfig
這個...
手動
Local Sys...
執行中
自動
Local Sys...
手動 (觸...
Local Sys...
啟動(S)
停止(O)
暫停(U)
繼續(M)
重新啟動(
所有工作(
重新整理(
內容(R)
說明(H)
已停用
Local Ser...
手動 (觸...
Local Sys...
手動 (觸...
Local Ser...
更新 Orchestrator 服務
管理 ...
執行中
手動
Local Sys...
打開【服務與應用程式】
點選【服務】
找到
【u000000】這種服務
按滑鼠右鍵，點選【內容】

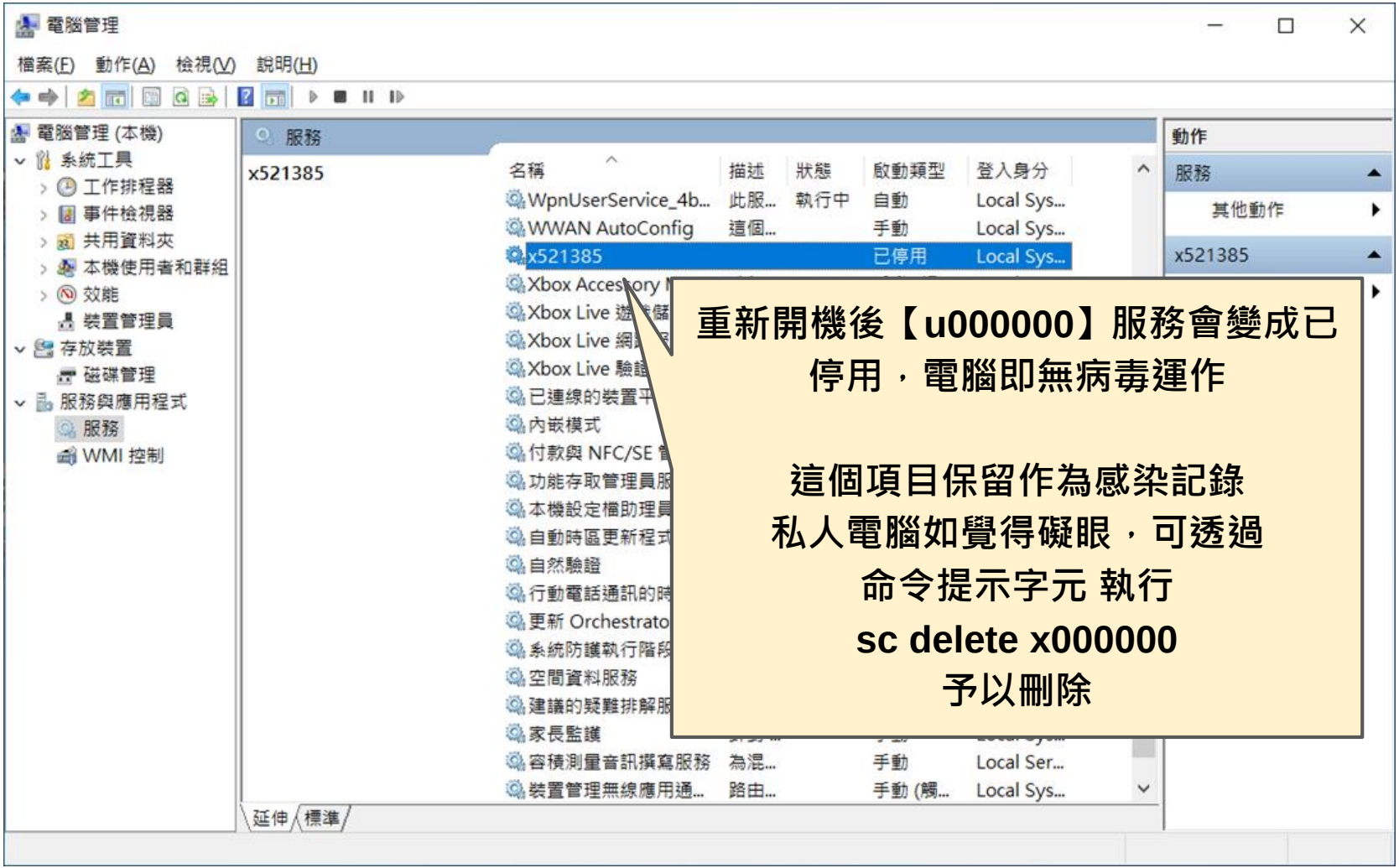

將【x000000】啟動類型改為【已停用】
x450853 內容 (本機電腦)
一般
登入
復原
相依性
x450853
x450853
C:\Windows\System32\svchost.exe -k DcomLaunch
啟動類型(E):
已停用
自動 (延遲啟動)
自動
手動
已停用
服務狀態:
執行中
啟動(S)
停止(T)
暫停(P)
繼續(R)
您可以在這裡指定啟動服務時所要
啟動參數(M):
確定
取消
套用(A)
將【u000000】服務停止

請下載 cure.zip 小工具，解壓縮密碼為 0000
https://drive.google.com/file/d/1_jhAqGSMTdQKIcDaJMs_uwzLrMu27w-t/view?usp=sharing



1. cure
請按滑鼠右鍵，以系統管理員身份執行，這個程序會刪除所有病毒生成的檔案

2. console
直接執行，這個程序會刪除病毒在系統登錄檔增加的資料


電腦管理
檔案(F) 動作(A) 檢視(V) 說明(H)
電腦管理 (本機)
系統工具
工作排程器
事件檢視器
共用資料夾
本機使用者和群組
效能
裝置管理員
存放裝置
磁碟管理
服務與應用程式
服務
WMI 控制
服務
x521385
名稱 描述 狀態 啟動類型 登入身分
WpnUserService_4b... 此服... 執行中 自動 Local Sys...
WWAN AutoConfig 這個... 手動 Local Sys...
x521385 已停用 Local Sys...
動作
服務
其他動作
x521385
重新開機後【u000000】服務會變成已停用，電腦即無病毒運作
這個項目保留作為感染記錄
私人電腦如覺得礙眼，可透過
命令提示字元 執行
sc delete x000000
予以刪除
延伸 標準