

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

The screenshot shows a Windows File Explorer window with the address bar set to '222 (I:)'. The left sidebar shows the navigation pane with '本機' (This PC) selected. The main pane displays a table of files and folders:

名稱	修改日期	類型
114		資料夾
NXT		資料夾
康軒		資料夾
222	2025/2/11 上午 10:42	捷徑

Two callout boxes are present:

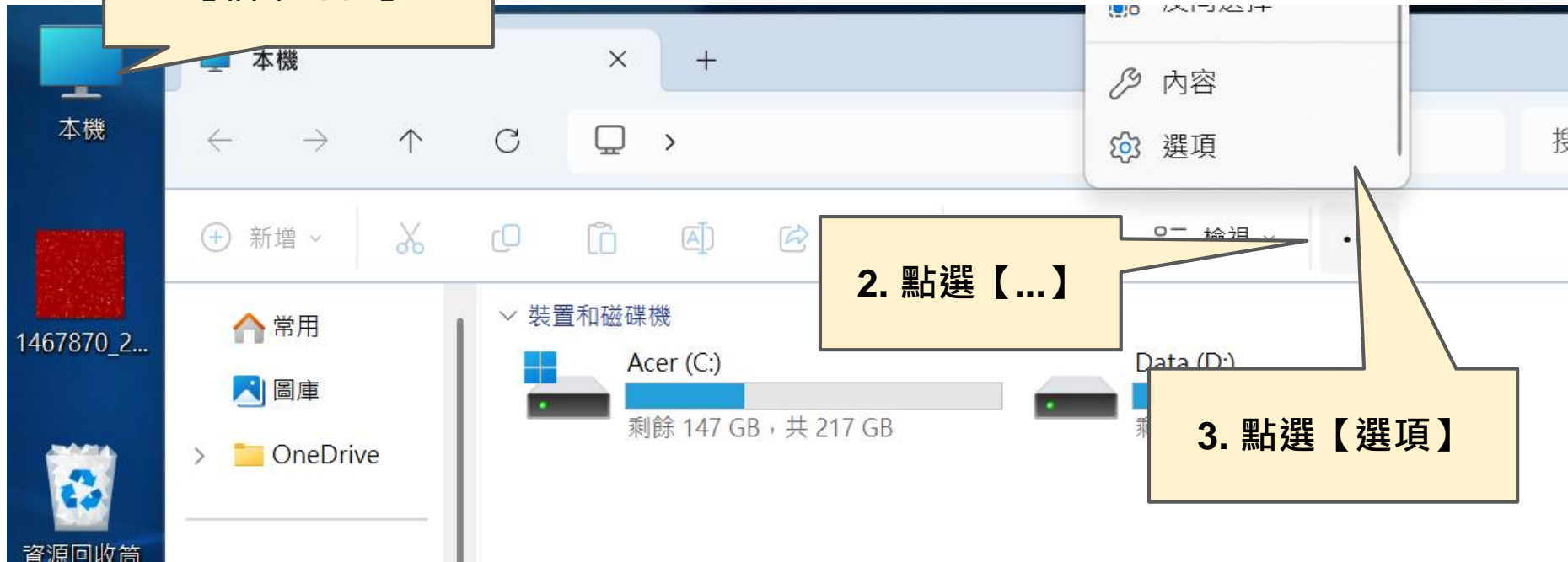
- A callout box pointing to the '222' entry in the table contains the text: "隨身碟如已中毒，只會看到一個捷徑，看不到原本的檔案。"
- A callout box pointing to the '222' entry contains the text: "千萬不要點這個捷徑，他會造成電腦中毒，再感染其他隨身碟。"

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

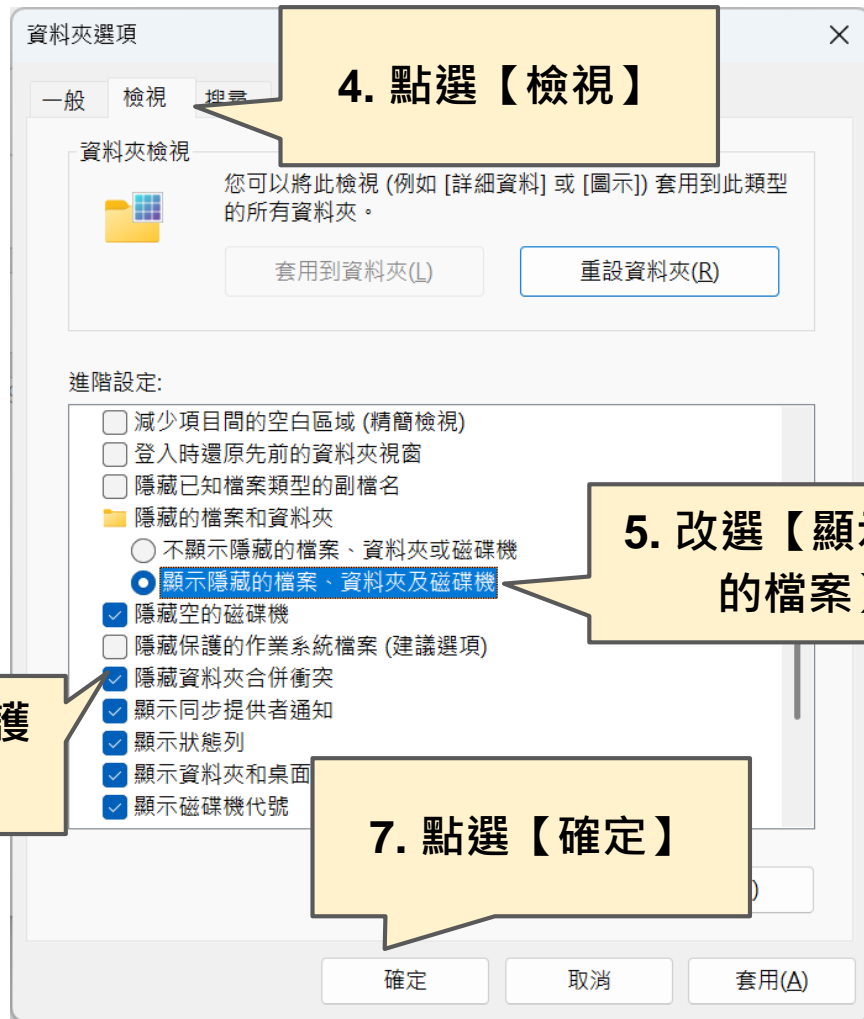
準備工作：讓病毒檔案現形

1. 打開【本機】或是【檔案總管】



2. 點選【...】

3. 點選【選項】



4. 點選【檢視】

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】

開啟中毒的隨身碟

The screenshot shows a Windows File Explorer window with the address bar set to '本機 > 222 (E:)'. The search bar contains the text '搜尋'. The ribbon includes icons for Home, Share, and Delete, along with '排序' (Sort), '檢視' (View), and '退出' (Exit) options. The main area displays a table of files and folders:

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

Two callout boxes provide instructions:

- 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

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
System Volume Information	2025/2/11 上午 10:37	檔案資料夾

3. 隨身碟檔案都藏在這裡，打開他

這是 Windows 工作的資料夾，不用理他

222

← → ↑ ↻ > 本機 > 222 (E:) > 222 搜尋 222

新窗 剪貼 複製 貼上 刪除 排序 檢視 詳細資料

名稱	修改日期	類型	大小
113(1)2上ch1.pptx	2025/2/12 上午 10:10	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		AT 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 .docx	2025/2/12 上午 09:28	Microsoft Word 文件	1,141 KB

4. 全選檔案 (可以按 **Ctrl+A**) , 然後【剪下】

5. 回到上一頁

9 個項目 | 已選取 9 個項目 14

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	2024/9/6 上午 10:18	Microsoft PowerPoint 檔案	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	2025/2/12 下午 12:27	Microsoft Word 文件	2,697 KB
新文字文件.txt	2025/2/12 上午 09:31	文字文件	0 KB
新增 Microsoft Excel 工作表.xlsx	2025/2/12		7 KB
電腦正常狀態 (1).docx	2025/2/12		1,184 KB
電腦正常狀態.docx	2025/2/12		1,141 KB

賀！清毒成功！

到這裡應該只剩兩個資料夾

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
System Volume Information	2025/2/11 上午 10:37	檔案資料夾

1. 隨身碟檔案都藏在這裡，打開他

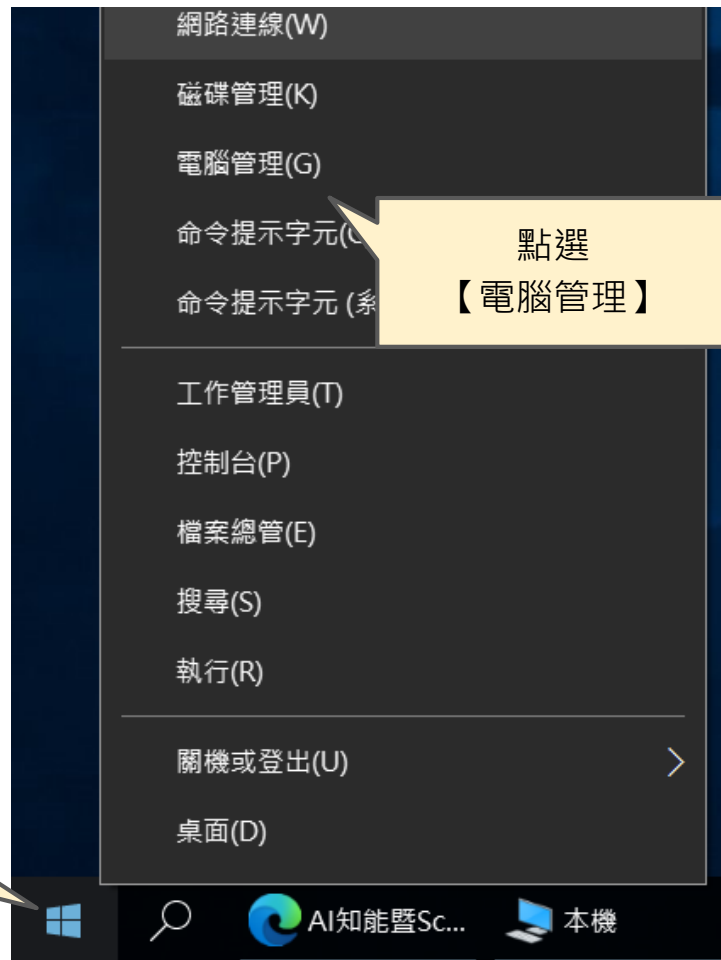
這是 Windows 工作的資料夾，不用理他

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。

在【開始】按鈕
按右鍵



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

服務

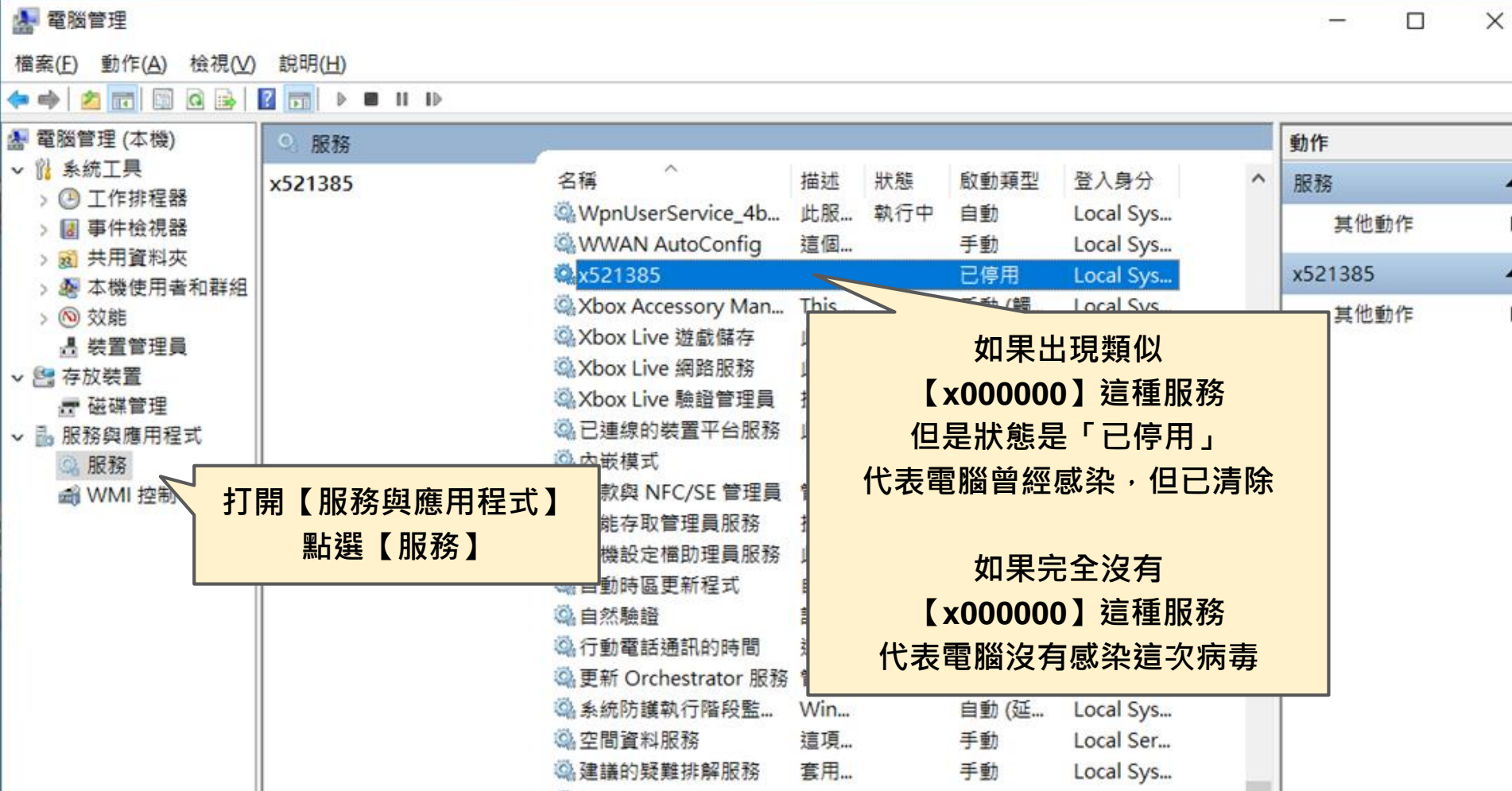
x450853

[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...	執行中	手動	Local S...
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...

打開【服務與應用程式】
點選【服務】

如果出現類似
【x000000】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 (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

打開【服務與應用程式】
點選【服務】

名稱	描述	狀態	啟動類型	登入身分
x521385		已停用		Local Sys...
WpnUserService_4b...	此服...	執行中	自動	Local Sys...
WWAN AutoConfig	這個...		手動	Local Sys...
Xbox Accessory Man...	This...	已停用 (備...		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				
機設定權助理員服務				
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...

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

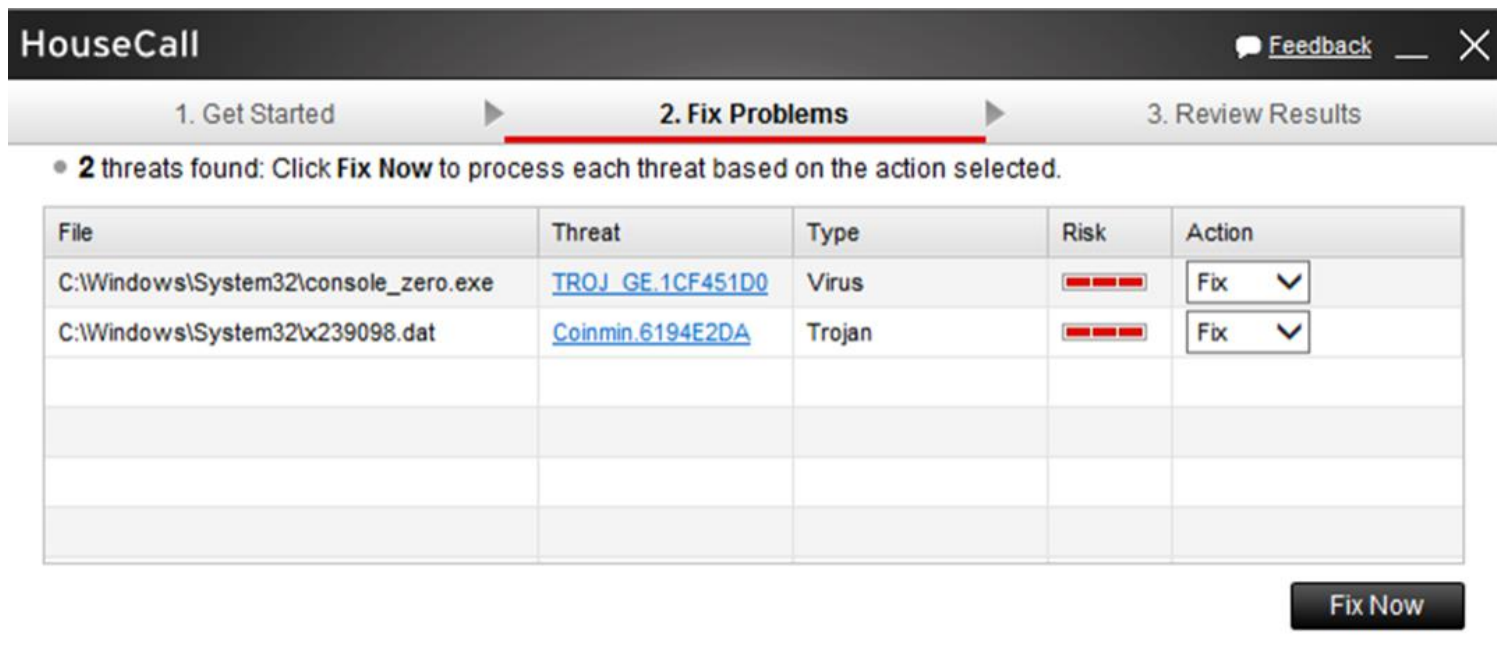
如果完全沒有
【x000000】這種服務
代表電腦沒有感染這次病毒

動作
服務
其他動作
x521385
其他動作

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



The screenshot shows the HouseCall interface with three steps: 1. Get Started, 2. Fix Problems (highlighted with a red underline), and 3. Review Results. A message states: "2 threats found: Click Fix Now to process each threat based on the action selected." Below this is a table with the following data:

File	Threat	Type	Risk	Action
C:\Windows\System32\console_zero.exe	TROJ_GE.1CF451D0	Virus	High Risk (3 red bars)	Fix <input type="button" value="v"/>
C:\Windows\System32\x239098.dat	Coinmin.6194E2DA	Trojan	High Risk (3 red bars)	Fix <input type="button" value="v"/>

A "Fix Now" button is located at the bottom right of the interface.

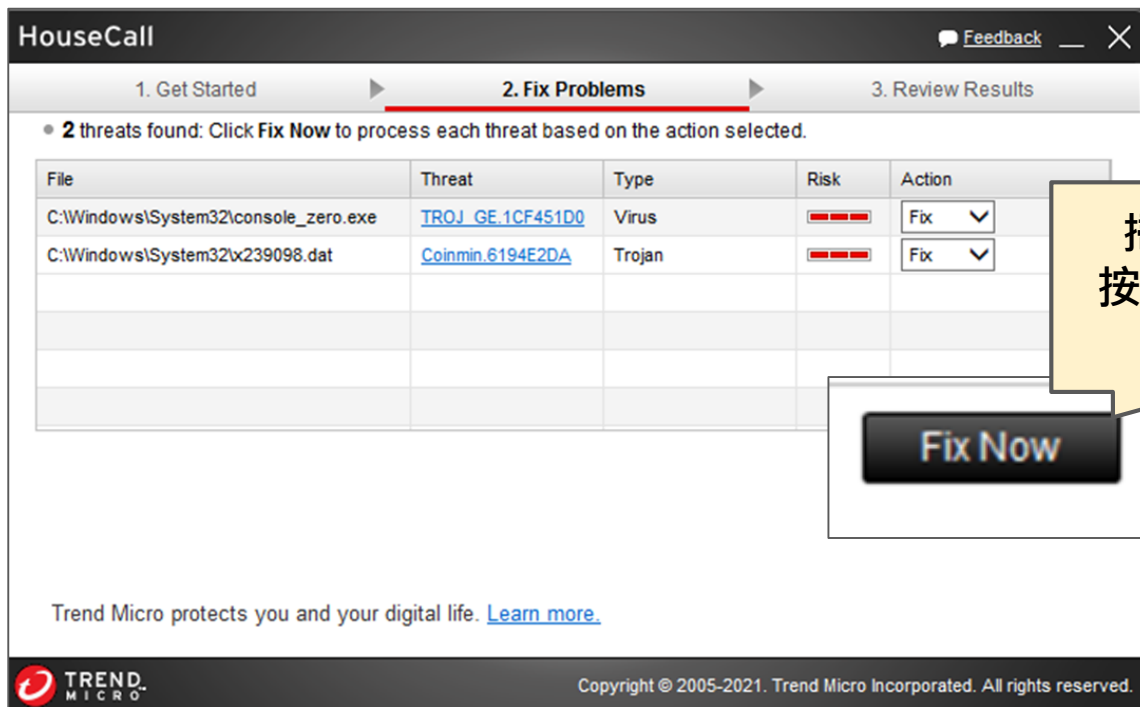
5. 如何清除電腦病毒？

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



The screenshot shows the HouseCall application window with the following content:

- Progress bar: 1. Get Started | **2. Fix Problems** | 3. Review Results
- Message: • 2 threats found: Click **Fix Now** to process each threat based on the action selected.
- Table of detected threats:

File	Threat	Type	Risk	Action
C:\Windows\System32\console_zero.exe	TROJ_GE.1CF451D0	Virus	High	Fix
C:\Windows\System32\x239098.dat	Coinmin.6194E2DA	Trojan	High	Fix

At the bottom of the interface, there is a prominent **Fix Now** button.

掃描完成後
按下 **Fix Now**
即可

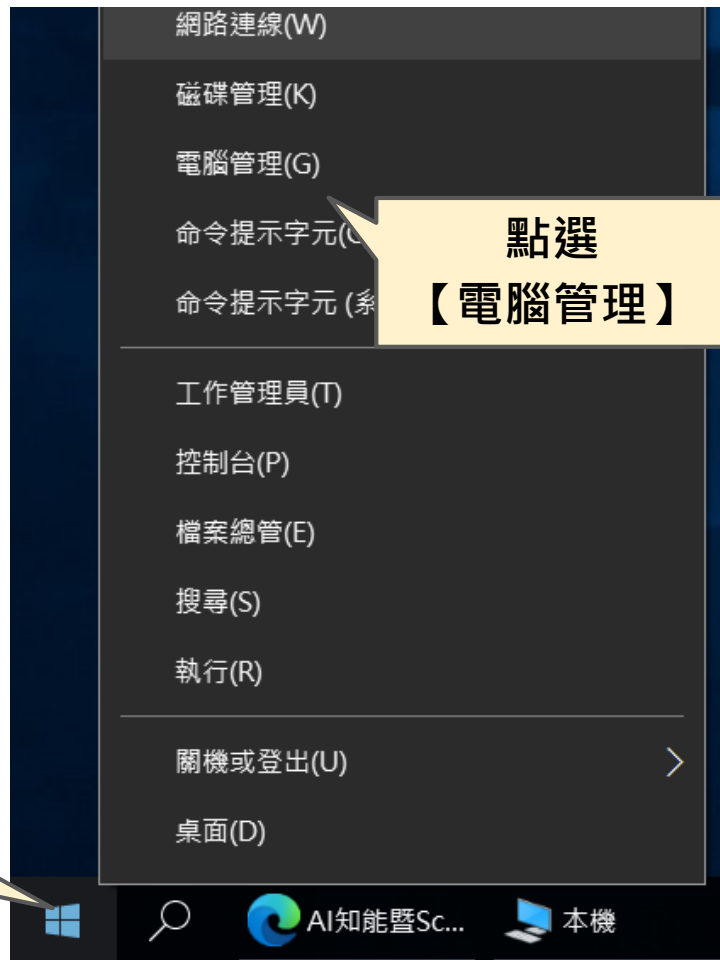
Fix Now

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**

在【開始】按鈕
按右鍵



The screenshot shows the Windows 'Computer Management' console. The left sidebar is expanded to 'Services and Applications' > 'Services'. The main pane shows a list of services. A service named 'x450853' is selected, and a context menu is open over it. A yellow callout box points to the 'Services and Applications' folder in the sidebar, and another yellow callout box points to the 'Content' option in the context menu.

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
 - Windows 更新

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...
x450853		執行中	自動	Local Sys...
Xbo...	3 ...		手動 (觸...	Local Sys...
Xbo...	P		手動 (觸...	Local Sys...
Xbo...				
Xbo...				
已連				
內嵌				
付款	所有工作...			
功能				
本機				
自動				
自然	先...		手動 (觸...	Local Sys...
行動	頁...		手動 (觸...	Local Ser...
更新 Orchestrator 服務	管理 ...	執行中	手動	Local Sys...

找到
【x000000】這種服務
按滑鼠右鍵，點選【內容】

打開【服務與應用程式】
點選【服務】



將【x000000】啟動類型
改為【已停用】

將【x000000】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_jhAqGSMTdQKlcDaJMsuwzLrMu27w-t/view?usp=sharing



cure.bat

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



console.reg

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

名稱	描述	狀態	啟動類型	登入身分
x521385		已停用	已停用	Local Sys...
WpnUserService_4b...	此服...	執行中	自動	Local Sys...
WWAN AutoConfig	這個...		手動	Local Sys...
Xbox Accessory M...				
Xbox Live 遊...				
Xbox Live 網...				
Xbox Live 驗證				
已連線的裝置平				
內嵌模式				
付款與 NFC/SE 管				
功能存取管理員服				
本機設定權助理員				
自動時區更新程				
自然驗證				
行動電話通訊的時				
更新 Orchestrato				
系統防護執行階段				
空間資料服務				
建議的疑難排解服				
家長監護				
容積測量音訊撰寫服務	為混...		手動	Local Ser...
裝置管理無線應用通...	路由...		手動 (觸...	Local Sys...

動作

- 服務
- 其他動作

x521385

重新開機後【x000000】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