Helper. VBS 隨身碟病毒的解法(一)隨身碟解毒

隨身碟中毒時的狀態:原本所有檔案消失,只剩一個名稱為隨身碟廠牌型號的捷徑



請勿開啟捷徑,將隨身碟插入電腦不會造成電腦中毒,執行捷徑才會 請先至檢視功能表,將「隱藏的項目」打勾即可看到全部的目錄



原本隨身碟內所有檔案都會被病毒移到「_」這個目錄下,請自行將檔案移到根目錄下或備份到其他 地方,然後刪除「_」與WindowsServices 病毒目錄及根目錄下的捷徑,病毒清除完成。(System Volume Information 為系統目錄,不需處理)

Helper. VBS 隨身碟病毒的解法(二)電腦解毒

電腦中毒時,不會影響電腦本身檔案,只有在隨身碟插入時會將隨身碟上的檔案隱藏並將病毒寫入 隨身碟。請在工作列上按右鍵,選擇工作管理員,然後選擇「開機」標籤頁

805-x6		±₽901.msr AlPALand	oute listent Sulp
工具列(1)	>		
授导(H)	>		
✓ 展示 [工作检視] 按鈕(V)			
在工作列上顺示連結人(P)			
✓ 顧示 [Windows Ink 工作編] 按鈕(W)			
賬示構控式課營按鈕(Y)			
驟示虞面(S)			
工作管理局(K)			
✓ 鐵定工作列(L)			
口作列設定(1)			
		4	

		-	
開機 使用 詳細資料 朋	服務		
		最後一個 BIOS	時間: 10.3 秒
發行者	狀態	啟動影響	
Ulead Systems, Inc.	已停用	無	^
	已停用	無	
IVT Corporation	已啟用	低	
	已啟用	未測量	
Creative Technology Lt	已敵用	低	
Disc Soft Ltd	已啟用	高	
Dropbox, Inc.	已啟用	高	
Google	已啟用	高	
	已啟用	未測量	
Intel Corporation	已啟用	低	
	関機 使用 詳細資料 系 發行者 Ulead Systems, Inc. IVT Corporation Creative Technology Lt Disc Soft Ltd Dropbox, Inc. Google Intel Corporation	酸行音 取行音 以lead Systems, Inc. ご停用 ご停用 ご停用 ご停用 ご停用 ご作用 のでのする範囲 こ 和 の の の の の の の の の の の の の	構像 使用 詳細資料 服務 最後一個 BIOS 發行者 武種 叙動影響 Ulead Systems, Inc. 己停用 無 己停用 無 IVT Corporation 己叙用 係 己叙用 未測量 Creative Technology LL 己叙用 係 Disc Soft Ltd 己叙用 高 Dropbox, Inc. 己叙用 高 Google 己叙用 高 三叙用 未測量 Intel Corporation 己叙用 係

在開機程式中如果發現 helper.vbs 此項目,表示電腦已經中毒。請先到「處理程序」標籤頁,找到 圖中的兩個 microsoft windows based script host 程式,按右下角的「結束工作」。

1 N	工作管理員				- 🗆 🗡	
榴案(F) 選項(O) 檢視(V)						
處理程序 效能 應用程式歷程記錄 啟動 使用者 詳細資料 服務						
		9%	62%	2%	0%	
名稱	態	CPU	記憶體	磁碟	網路	
Hamachi Client Application (3		0%	1.7 MB	0 MB/秒	0 Mbps	^
Hamachi Client Tunneling Eng		0%	1.4 MB	0 MB/秒	0 Mbps	
🛃 Java Update Checker (32 位元)		0%	2.3 MB	0 MB/秒	0 Mbps	
🛃 Java Update Scheduler (32 位		0%	1.0 MB	0 MB/秒	0 Mbps	
LMIGuardianSvc		0%	1.1 MB	0 MB/秒	0 Mbps	
. Microsoft ® Windows Based		0%	1.4 MB	0 MB/秒	0 Mbps	
👝 Microsoft ® Windows Based		0%	2.3 MB	0 MB/秒	0 Mbps	
Microsoft Office Click-to-Run		0%	8.4 MB	0 MB/秒	0 Mbps	
▷ 🔏 Microsoft Windows Search 素		0%	29.3 MB	0 MB/秒	0 Mbps	
▷ 🔟 PnkBstrA.exe (32 位元)		0%	0.6 MB	0 MB/秒	0 Mbps	
Runtime Broker		0%	6.4 MB	0 MB/秒	0 Mbps	
🛐 SoftEther VPN		0%	4.7 MB	0 MB/秒	0 Mbps	
SoftEther VPN		0%	3.7 MB	0 MB/秒	0 Mbps	

回到「開機」標籤頁,在helper.vbs上按右鍵,選擇「開啟檔案位置」

👪 l 💽 👪 = l		WindowsServices		- 🗆 🗙
檔案 常用 共用	檢視			^ 🕐
□□ 預覽窗格 □□ 詳細資料窗格 瀏覽窗格	超大圖示	□ 分組方式 • 排序方式 □ 新増欄 • 計調整所有欄位至最適大小	 □ 項目核取方塊 ☑ 副檔名 ☑ 陽藏的項目 選取的 	▲ 選項 項目
窗格	版面配置	目前檢視	顯示/隱藏	
← → 本 → 泰曜 → AppData → Roaming → WindowsServices v C 授尋 WindowsServices / ●				
☆ 我的最愛 🔷	名稱	修改日期 類型	大小	
🗼 下載	📓 helper.vbs	2016/2/26 下午 0 VBScript 指:	令榴 2 KB	
■ 桌面	📓 installer.vbs	2016/2/26 下午 0 VBScript 指:	令檔 4 KB	
🧾 最近的位置 🝊 OneDrive	🛞 movemenoreg.vbs	2016/2/25 下午 0 VBScript 指:	令檔 2 KB	

目錄完整路徑為C:\Users\使用者名稱(每部電腦不一定相同)\AppData\Roaming\WindowsServices 請到上一層將WindowsServices 目錄移除。

最後到系統啟動目錄 C:\Users\使用者名稱(每部電腦不一定相

同)\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup,目錄下可以找到一個名為 Helper 的捷徑,請將之刪除,病毒清除完畢。