USB 病毒防治說明

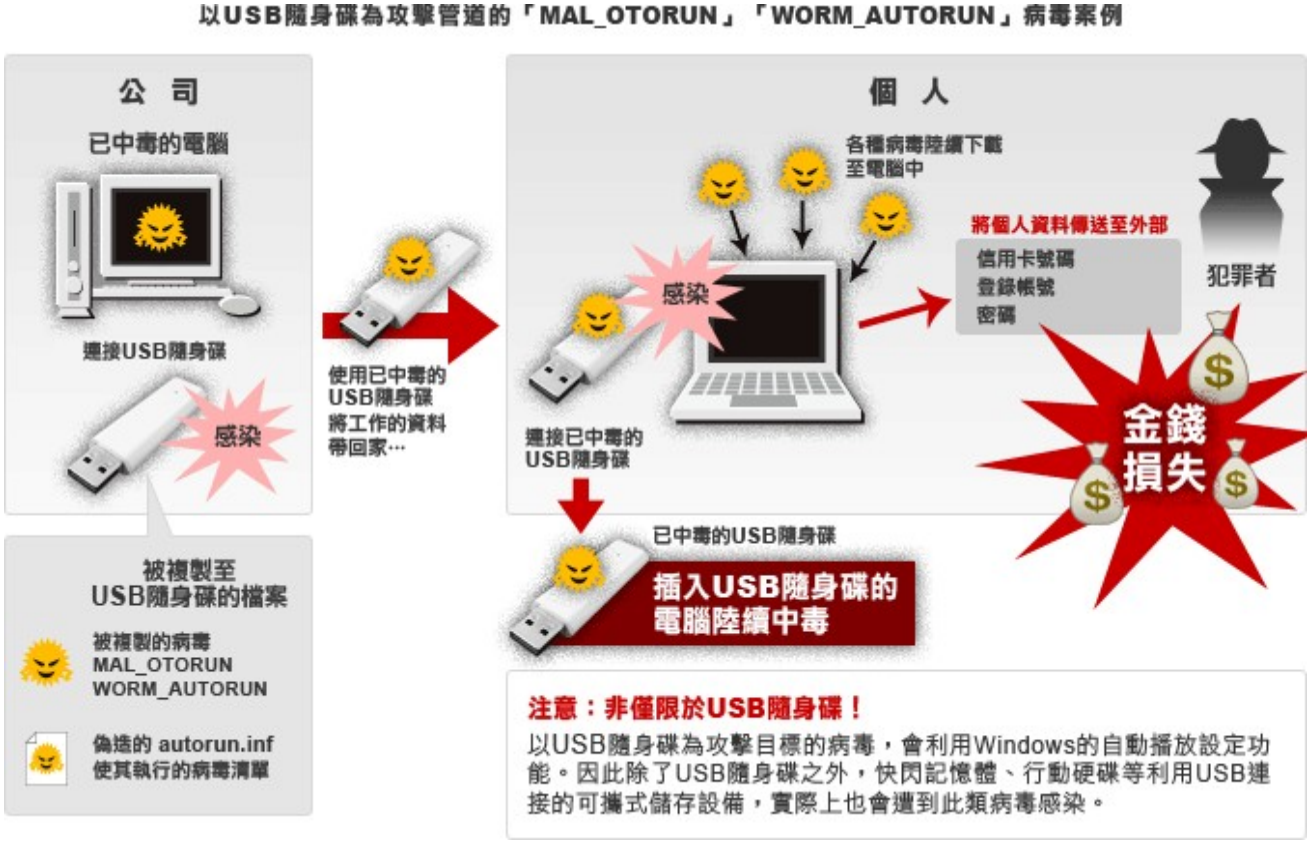
1、 USB 病毒說明：

所謂的 USB 病毒，就是 Autorun 病毒(自動執行病毒)，病毒透過 Autorun.inf 系統檔案在 USB 等支援熱拔插的週邊儲存裝置內(例即 USB 界面的姆指碟、光碟、USB 硬碟…)，然後當你每次插入電腦的時候它就會自動執行，即使你沒有去執行它，因為電腦的設定會自動執行 USB 裝置，所以你的電腦就會在不知不覺中中毒了！

Autorun.inf 是 Windows 作業系統(OS)的正常檔案，微軟當初在設計時為了能夠自動的播放光碟內容，因此透過 Windows 在偵測到有週邊裝置接到電腦主機上時，判斷該週邊裝置是否有 Autorun.inf，然後讀取 Autorun.inf 內指定的檔案進而達到自動播放的功能，認為 Autorun.inf 就是病毒的觀念是不正確的，事實上它是代罪羔羊。目前在市面上最常看到 Autorun.inf 的應用實例就是在幼教光碟上的自動播放。

2、 傳染方式：

USB 病毒的行為是隨著病毒作者的想法而有所不同，最常見的手法是病毒透過三個檔案互相配合運作：***病毒主程式(母程式 .exe; .com; .pif …)***、***子程式(.dll)***、***Autorun.inf 檔案***，惡意程式作者要確保病毒能夠帶來最大的效益，所以會在病毒被執行後，立刻搜尋電腦上所有的週邊裝置，並且在這些裝置上產生病毒自己的三個檔案，然後在母程式執行後自殺，透過子程式繼續監控電腦是否還有其他後來接到電腦上的週邊裝置，並且在 Autorun.inf 檔案被刪除之後，立刻再產生新的 Autorun.inf 檔案。



3、 預防與清除方式：

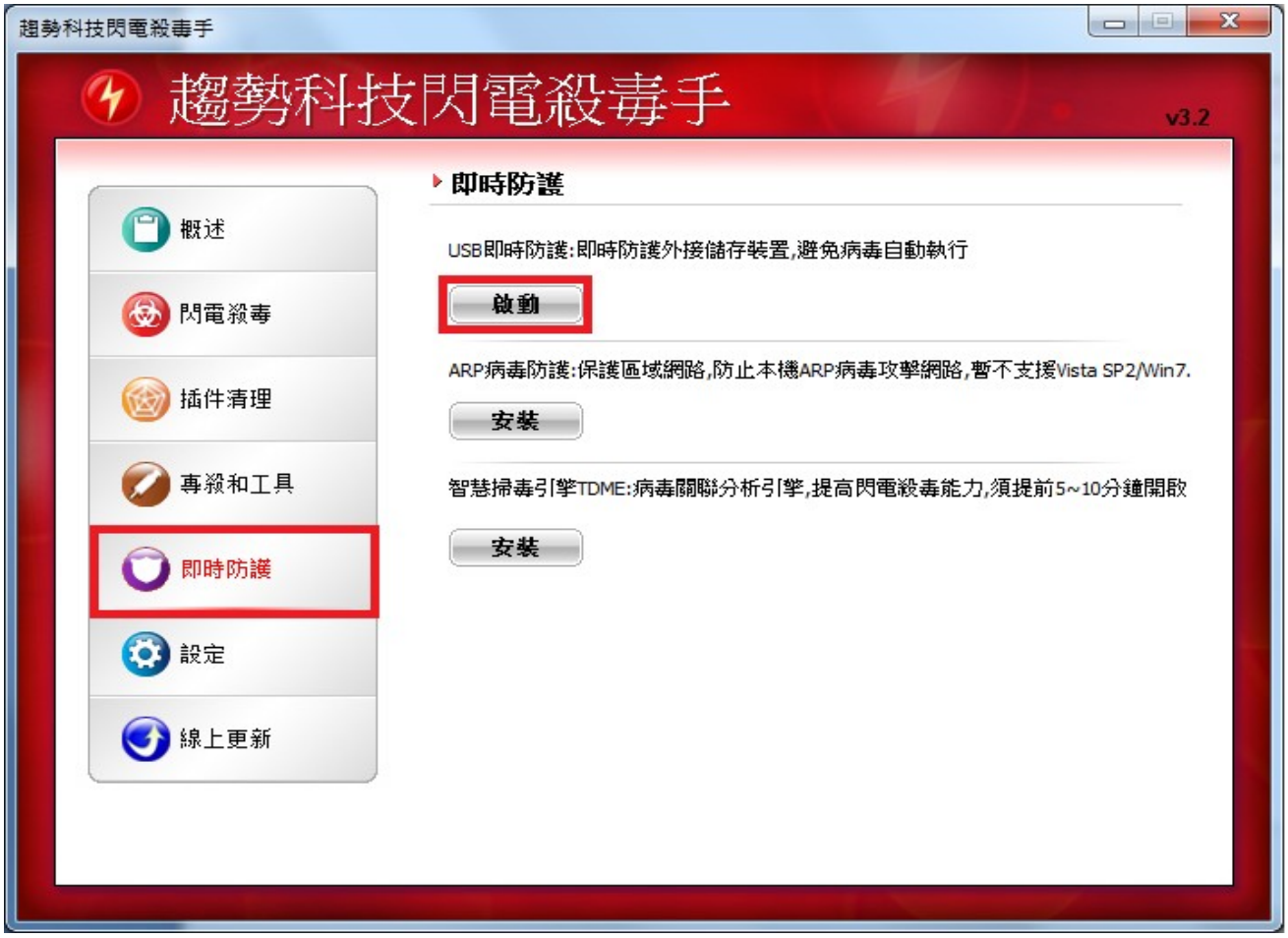
使用趨勢科技提供閃電殺毒手清除病毒軟體清除病毒：

軟體下載：登入 i-touch -> 電算中心 -> 電腦小幫手 -> 防毒系統安裝與說明網頁下載

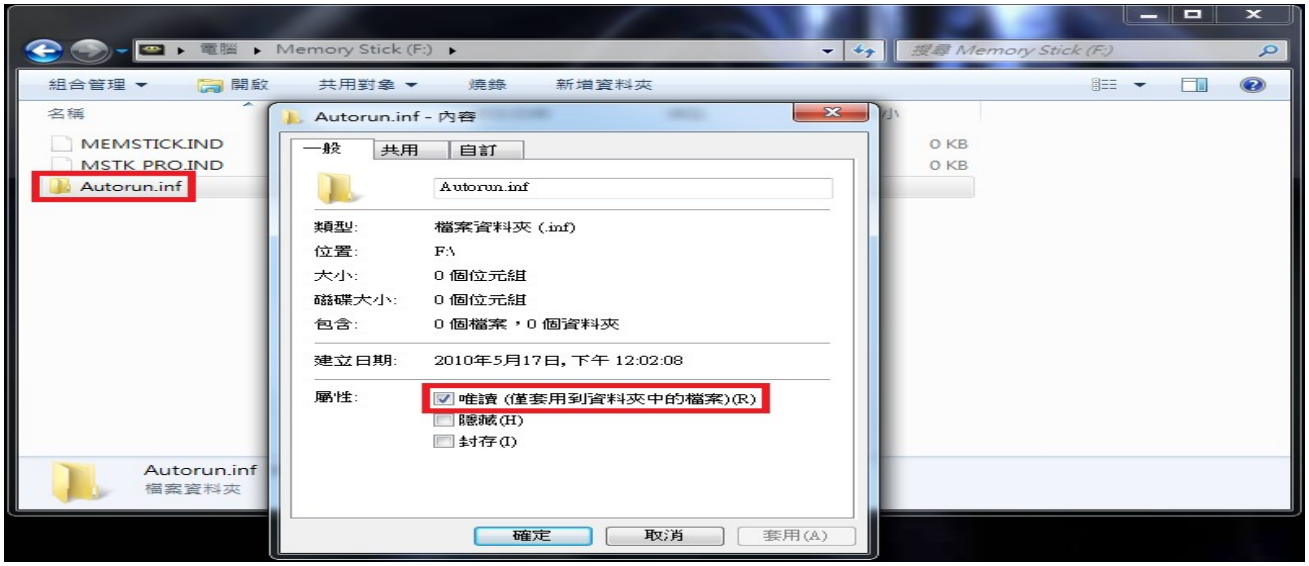
使用前，請先閱讀軟體使用說明文件，將軟體解壓縮並執行資料夾中的 ***LighteningCleaner.exe***，請您先點選到閃電殺毒，將週邊裝置加入到掃瞄清單中，再按開始掃描作業，如有發現惡意程式會將其列入清單，如確認清單中均為惡意程式時即可按開始清除進行病毒清除。

4、 PC 防護設定：

1. 使用閃電殺毒手建立反 Autorun.inf 自動執行：



2. 在所有的磁碟機中手動建立 Autorun.inf 資料夾，並設定唯讀權限，以避免病毒產生相同的檔案到週邊設備中。



但此種作法還是有限制。例如電腦主機的各磁碟都已新增 autorun.inf 的資料夾，而後接上有病毒的 USB 隨身碟時，Windows 系統還是會自動執行 autorun.inf，並載入相關病毒，到 C 磁

碟的Windows系統資料夾中，該電腦依然會中毒，然而當該病毒要寫入其他磁碟的根目錄時，因為這些地方都已經存在autorun.inf資料夾，而無法感染，中毒範圍僅局限在Windows系統資料夾中。若將沒有感染且有autorun.inf資料夾的USB儲存裝置也設定。連接到遭感染的電腦時，因為本身已存在資料夾，也將無法載入病毒。需要注意的是，上述方式僅防範病毒利用autorun.inf自動執行的功能，若使用者不慎點選而執行了病毒檔，還是會中毒。

★*錯誤觀念：先按著Shift鍵不放，再連接USB隨身碟等週邊設備，這個方法是沒有用的，按住SHIFT不放是關閉電腦的「自動撥放」，而不是「自動執行」，自動撥放是插入隨身碟後通常會跑出一個介面讓你選擇你要做的事情（例如音樂，看資料夾，看圖等）而自動執行是電腦會自動開啟程式。*