義守大學圖書與資訊處

工作聯繫單

致：全校教職員生　　（104）圖資字第 030 號

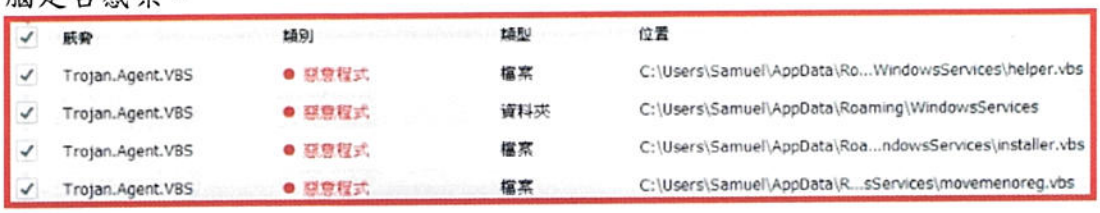
□請覆　■免覆　　日期：105 年 6 月 8 日

主旨：近日校園發現的 USB 隨身碟病毒，**自我檢查與感染後手動處理**相關資訊，請 查照。

說明：

一、 自我檢查方法：

(一) 電腦檢測：WIN 鍵+R 開啟**執行**視窗→鍵入「shell:startup」後按 Enter，即打開檔案總管並停留在**啟動(startup)**目錄→請檢查系統目錄是否有 “helper” 的捷徑，即可概略判定電腦是否感染。



威脅	類別	類型	位置
Trojan.Agent.VBS	惡意程式	檔案	C:\Users\Samuel\AppData\Ro...WindowsServices\helper.vbs
Trojan.Agent.VBS	惡意程式	資料夾	C:\Users\Samuel\AppData\Roaming\WindowsServices
Trojan.Agent.VBS	惡意程式	檔案	C:\Users\Samuel\AppData\Roa...ndowsServices\installer.vbs
Trojan.Agent.VBS	惡意程式	檔案	C:\Users\Samuel\AppData\R...sServices\movemenoreg.vbs

(二) 隨身碟檢測：隨身碟內原有檔案消失，只剩餘與隨身碟設定名稱相同的捷徑，即可概略判定隨身碟是否感染。

二、 感染病毒後手動處理方式：

(一) 電腦方：

1. 請開啟電腦隱藏檔為可見：資料夾與搜尋選項→檢視→隱藏檔案和資料夾→選取 “顯示隱藏的檔案、資料夾及磁碟機”。
2. WIN 鍵+R 開啟**執行**視窗→鍵入「shell:startup」後按 Enter 檢查系統**啟動**目錄是否有 “helper” 的捷徑，若有代表該電腦已被植入程式。
3. 由 “helper” 的捷徑上按右鍵查詢捷徑的路徑，會找到一個[**WindowsServices**]的資料夾，裡面會有 3 個 **vbs** 所寫的檔案，將其刪除即可。
4. 重新開機後再執行第 2 步驟，刪除**啟動**目錄內“helper”的捷徑即可。

(二) 隨身碟方：

1. 請開啟電腦隱藏檔為可見：資料夾與搜尋選項→檢視→隱藏檔案和資料夾→選取 “顯示隱藏的檔案、資料夾及磁碟機” 。
2. 至隨身碟找到[_]資料夾，裡面即為隨身碟內原有檔案，將資料搬出即可。
3. 將隨身碟名稱相同捷徑刪除或進行隨身碟格式化。

三、 若使用本校校級電腦教室之電腦前，**建議先執行重新開機動作**，將電腦還原為原始狀態，以確保不受上一位使用者可能帶原之病毒感染。

四、 隨身碟病毒多有變種，如有相近，請參考此方法。

圖書與資訊處　資訊應用組
郭豐有　分機：2783　E-mail：isustuu04@isu.edu.tw

承辦人	二級主管	一級主管
圖書與資訊處 資訊應用組 約用專案助理 郭豐有 0608	圖書與資訊處 資訊應用組 組長 鍾美惠 0608	圖書與資訊處 處長 沈季燕 0608