

System.wSf 惡意程式手動移除全紀錄

1. 緣起

中正國中資訊組長表示，自從教務主任 2016 年某天去了教研中心 R206 開會，將隨身碟插入公用電腦，再攜回學校後，這隻惡意程式就在學校的各電腦流竄。感染的電腦或隨身碟，檔案或目錄都變成捷徑。去年我有提供 **usb virus killer** 程式，卻發現無法完全移除。

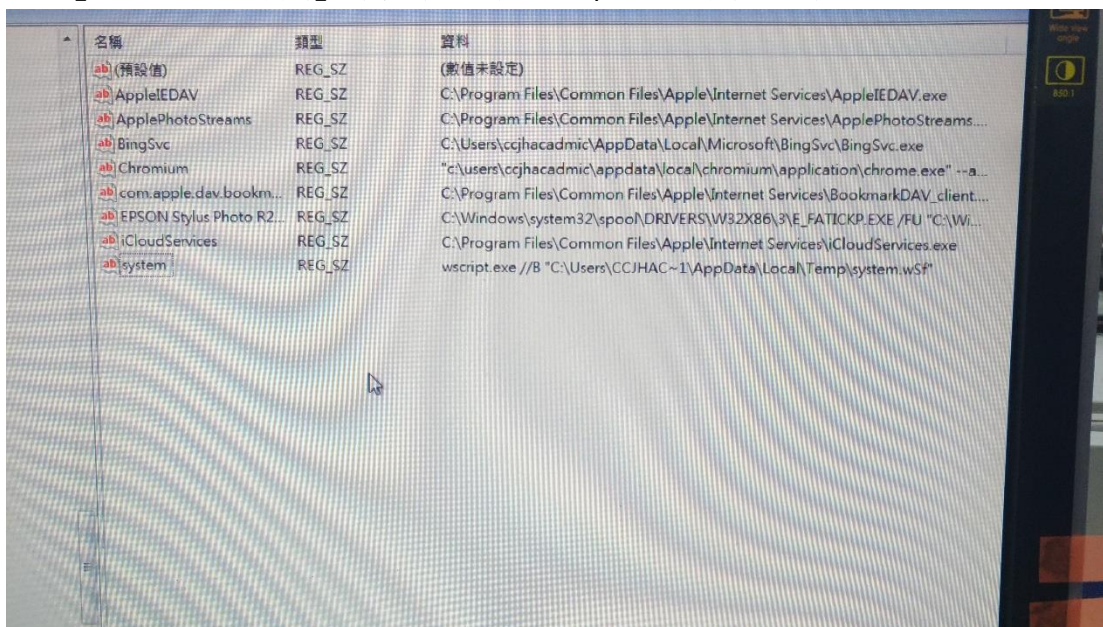
2. 傳播途徑

初步判斷會經由隨身碟拔插電腦的方式傳播，而且發現學校行政同仁的電腦，應該都沒有關閉 **autorun**。

3. 移除方式

3.1 **Ctrl + Alt + Del** 進入工作管理員，看一下執行緒中是否存在 **wscript**，如果有，強制停止。

3.2 於命令提示字元，輸入 **regedit**，再以系統管理員身份執行，點擊「編輯」，再點擊「尋找」，輸入關鍵字 **wscript.exe**，找到如下的畫面：



3.3 於上圖登錄檔 **System** 處，點擊滑鼠右鍵，點擊刪除，將該登錄機碼整個移除。

3.4 再次於 **Regedit** 尋找關字串 **wscript.exe** (或 **wscript**)，如果有發現如 3.2 所示的登錄機碼，不要客氣，全部刪除。

3.5 於命令提示列或是檔案總管，移轉 (**cd**) 目錄至 **c:\使用者\使用者名稱\AppData\Roaming\Microsoft\Windows\Start Menu\啟動** 看看是否存在 **system.wSf**，如果有，移除。上列目錄可能是隱藏的。

3.6 於命令提示列或是檔案總管，移轉 (**cd**) 目錄至 **c:\使用者\使用者名稱\AppData\Local\Temp** 看看是否存在 **system.wSf**，如果有，移除。上列目錄可能是隱藏的。

4. 病毒分析







- 4.1 System.wsf 其實是個以 VBScript 撰寫的小程式，但如果使用 notepad 開啟，會發現其中充斥著 XOXOX 或 101010 等字串，很顯然這個程式經過加密。
- 4.2 Wscript.exe 是 Windows 7 以後，內建在系統中用來執行 Vbscript 的程式，用途最多的就是 Office 套裝軟體中，用來呼叫外部以 VBScript 函式，在 Office KMS 驗證時也會用到。
- 4.3 現場觀察發現這支惡意程式就是利用系統 AutoRun 未關閉的漏洞進行傳播，但鑒於 VBScript 的特性，可透過 Office 開啟特定的檔案（可將 System.wsf 嵌入 Word、Excel）中，感染 Office 檔案，而 VBScript 程式也可嵌在網頁上，透過掛馬的方式，讓瀏覽器在不知不覺中下載到電腦中，達成感染的目的。故可判定這是一種具多形病毒特性，又透過系統本身漏洞傳播的木馬程式。
- 4.4 受限於現場時間與工具有限，無法側錄下受害主機 TCP Session，故無法判斷此惡意程式是否有透過特定的 TCP port 與外部主機通連，如果有此特性，就算是 BOTS 了！會這樣懷疑是因為本程式的作者費了一點心思設計多形模式（加密）以規避防毒軟體的掃描，想必不只有想感染隨身碟而已。
- 4.5 將病毒樣本上傳上 VirusTotal，經全球 68 個掃毒引擎分析的結果，只有 6 個認為它是惡意程式（MaleWare）的特性，如下：

system.wsf

The file system.wsf has been detected as malware by 6 anti-virus scanners. It runs as a scheduled task under the Windows Task Scheduler named ScriptGegX triggered daily at a specified time.

File name:	system.wsf
MD5:	9fe2b986fd8ac2958c49656c42f5e084
SHA-1:	96701f07de58bd36db8b48dc2c5e0fce2b8b2ce1
SHA-256:	00575c0d754f4537f7f8db42f891a65bb1c7bdcb5b2f805ba466d479075dc649

Analysis

Scanner detections:	6 / 68	
Status:	Malware	
Analysis date:	2/18/2017 4:47:45 AM UTC (a few moments ago)	
Scan engine	Detection	Engine version
 Avira AntiVirus	TR/Patched.Gen	7.11.30.172
 Dr.Web	infected with VBS.DownLoader.540	9.0.1.05190
 Emsisoft Anti-Malware	Trojan.VBS.Downloader.KI	10.0.0.5366
 F-Secure	Trojan.VBS.Downloader.KI	5.15.21
 Norman	Trojan.VBS.Downloader.KI	11.01.2016 17:30:26
 Sophos	Virus 'VBS/DwnLdr-NBU'	5.22

- 4.6 承上，難怪多數的防毒軟體無法偵防，更遑論掃除，只能手動移除之。