偽裝成系統檔案的
USB 隨身碟病毒分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

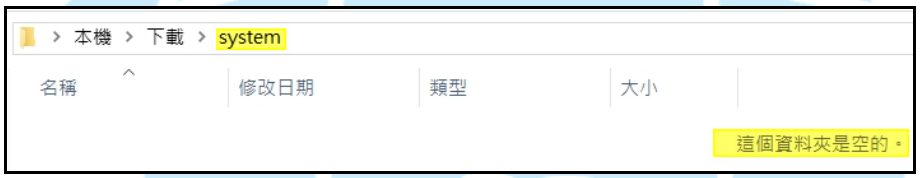
2020 年 05 月

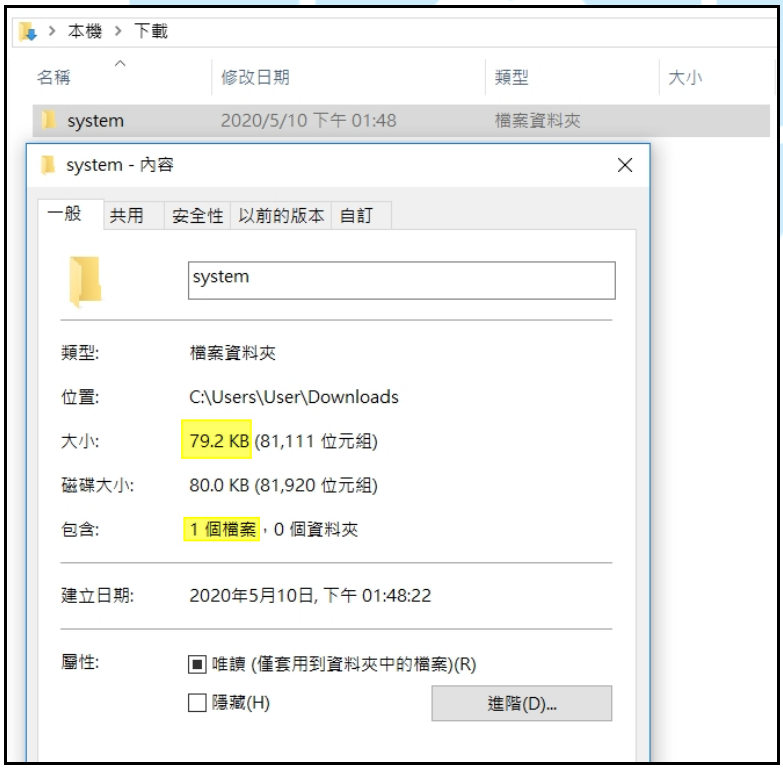
一、事件簡介

1. 2020 年 5 月初 TACERT 接獲外部情資提供一個在公務機關常見的隨身碟病毒，該病毒會使插入主機的隨身碟內檔案全部變成捷徑檔，而且防毒軟體偵測不到它的存在。
2. 為了瞭解該病毒的攻擊行為與對受害者的危害程度，本中心對病毒樣本進行檢測。

二、事件檢測

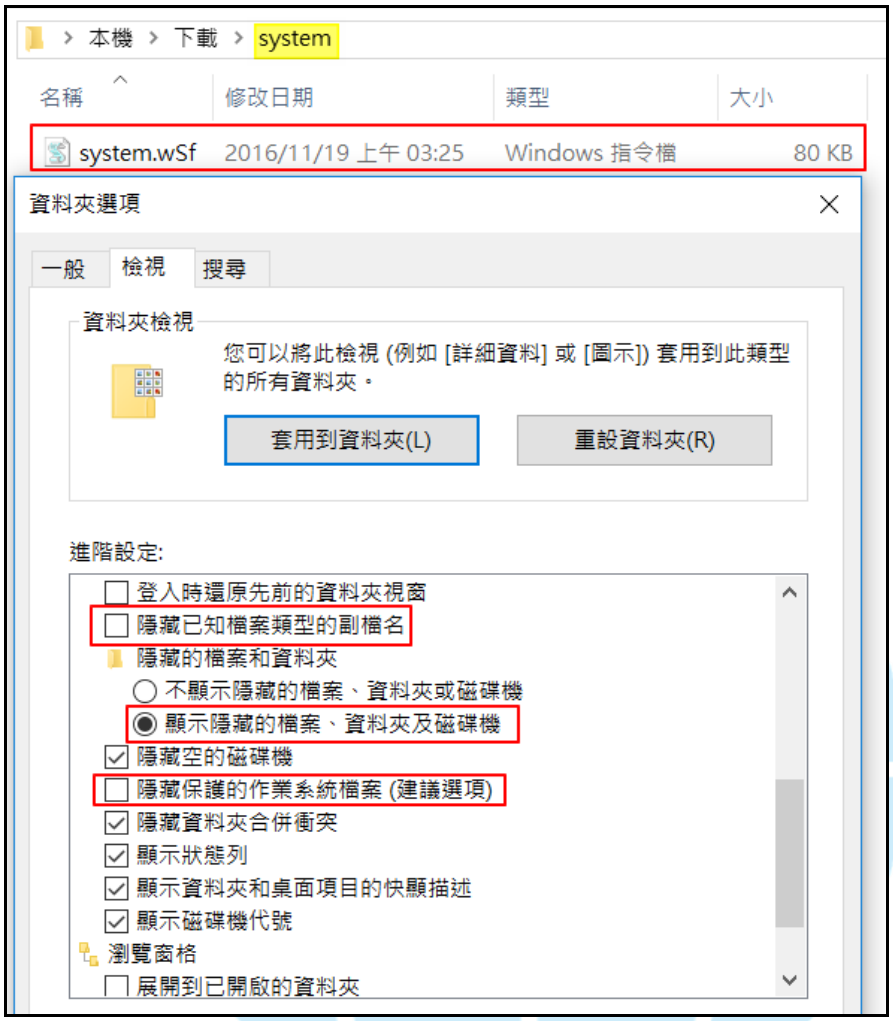
1. 首先，使用一台 32 位元 Windows 10 作業系統的虛擬機，將病毒樣本 system.zip 解壓縮後產生一個 system 資料夾，查看此資料夾未看到任何檔案在資料夾內，但是資料夾內容標示有一個 79.2KB 的檔案存在資料夾內。



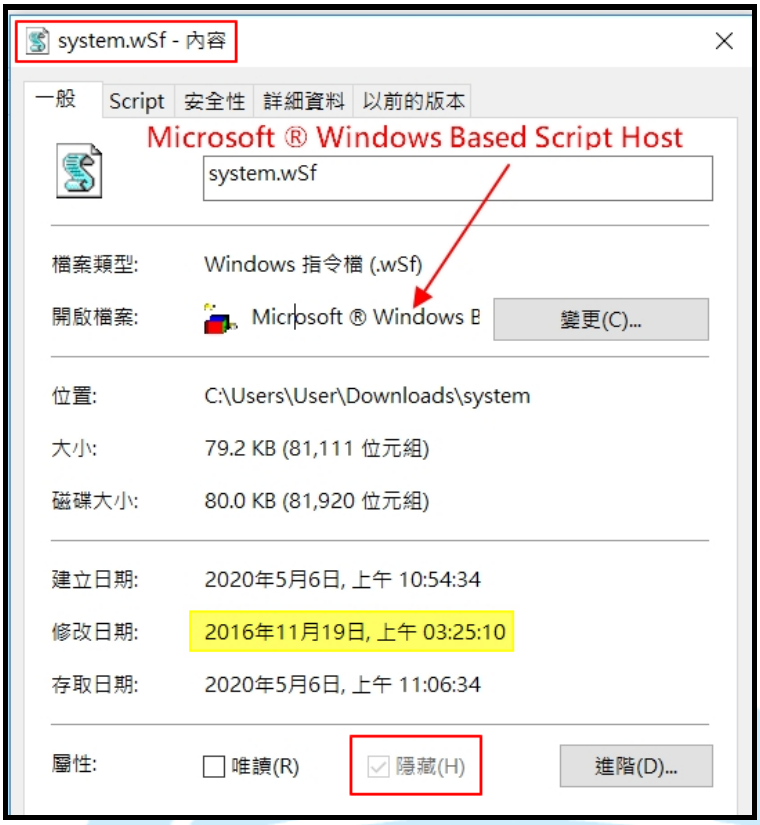


2. 經檢視「資料夾選項」的設定，發現除了不勾選「隱藏已知檔案類型的副檔

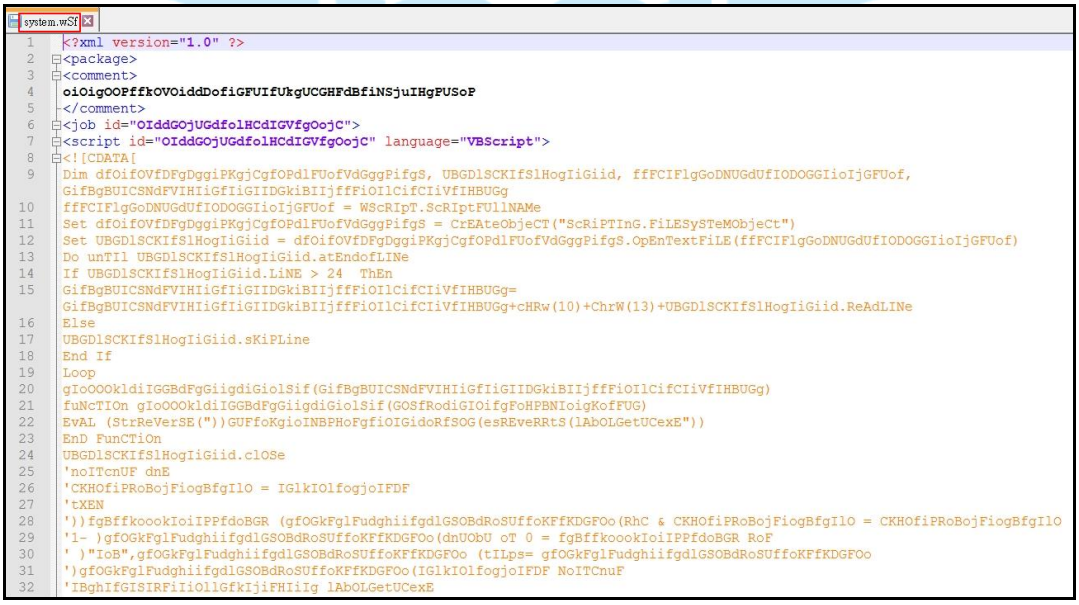
名」與設定「顯示隱藏的檔案、資料夾及磁碟機」以外，必須不勾選「隱藏保護的作業系統系統檔案(建議選項)」才能看到 system 資料夾內的檔案 system.wsf。

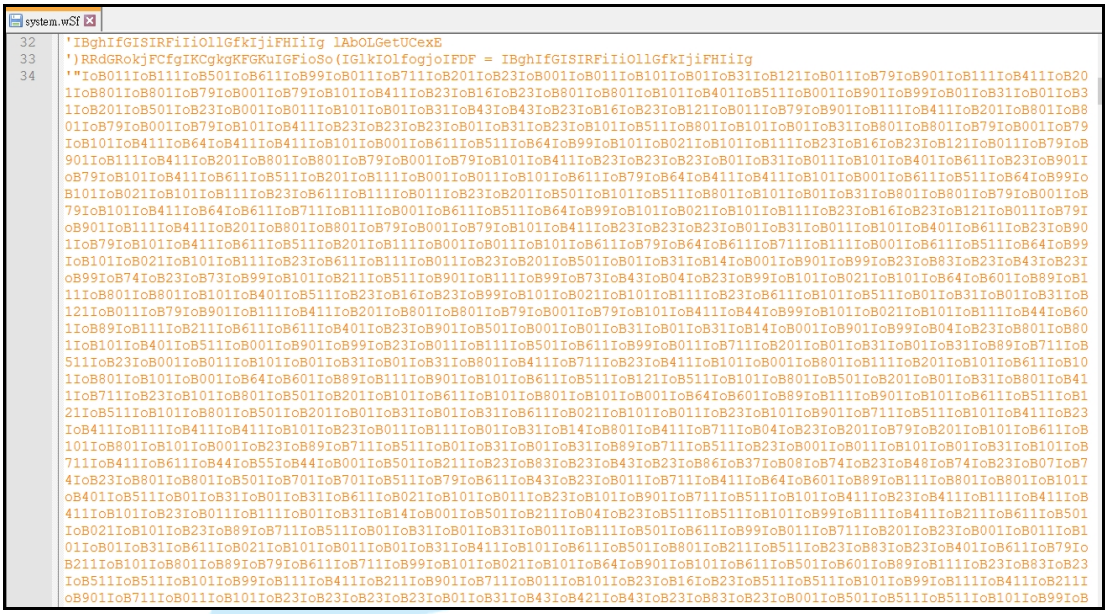


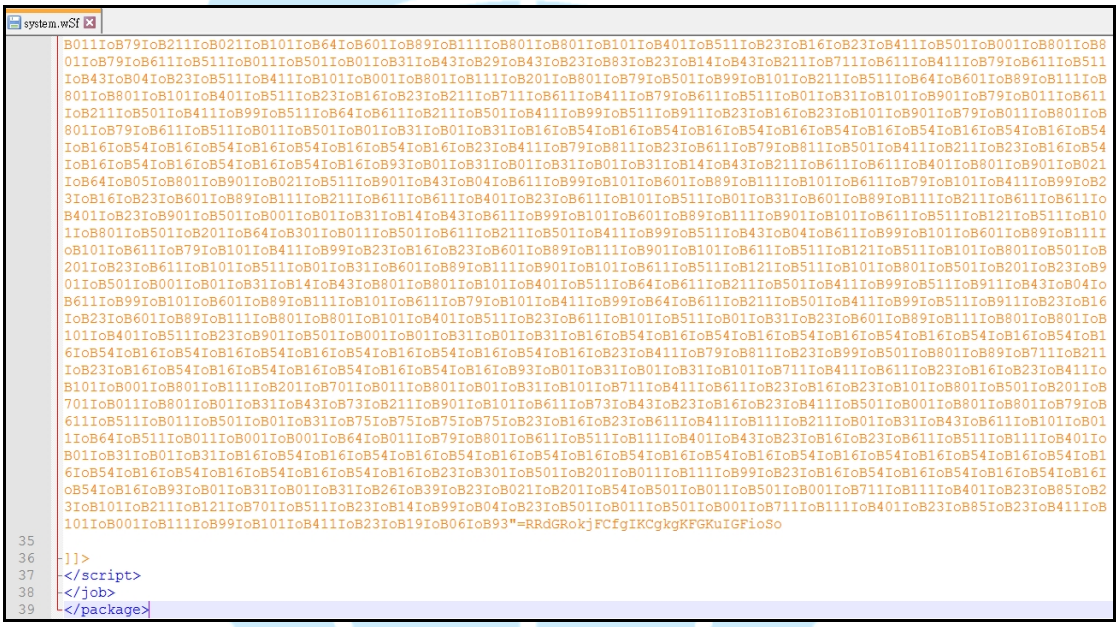
3. system.wSf 為一個 Windows 指令檔，可用 Microsoft Windows Based Script Host 開啟執行。由副檔名.wSf 得知此為 VB Script，它可被用來自動地完成重複性的 Windows 作業系統任務。在 Windows 作業系統中，VBScript 可以在 Windows Script Host 的範圍內執行。Windows 作業系統可以自動辨認和執行*.VBS 和 *.WSF 兩種檔案格式。另外，由檔案的修改日期 2016 年 11 月 19 日上午 03:25 得知該檔案非近期才出現的惡意程式。



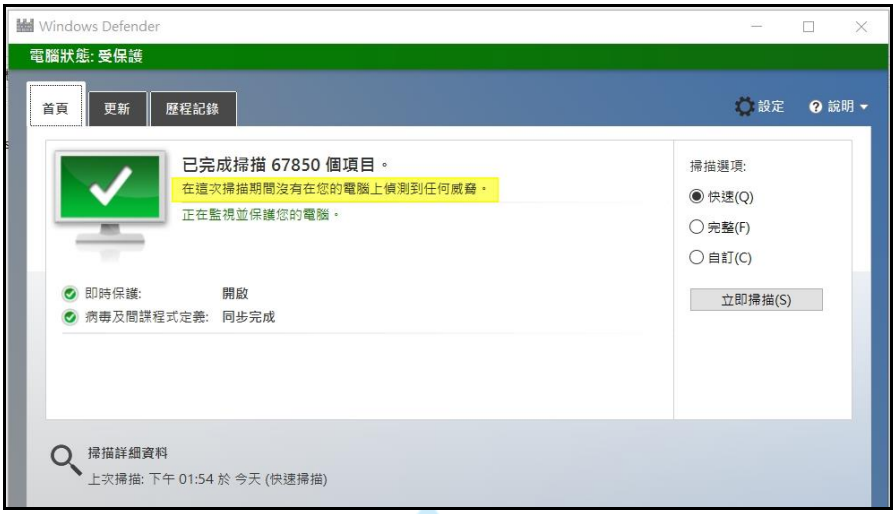
4. 以 Notepad++開啟 system.wSf 並檢視其內容，發現為一個 VB Script 所撰寫的亂碼程式。在 VB Script 語法中，有許多參數都使用一長串的亂碼表示，而且在程式碼最後以一大段亂碼結尾，讓瀏覽者無法解讀該程式的主要用途為何。

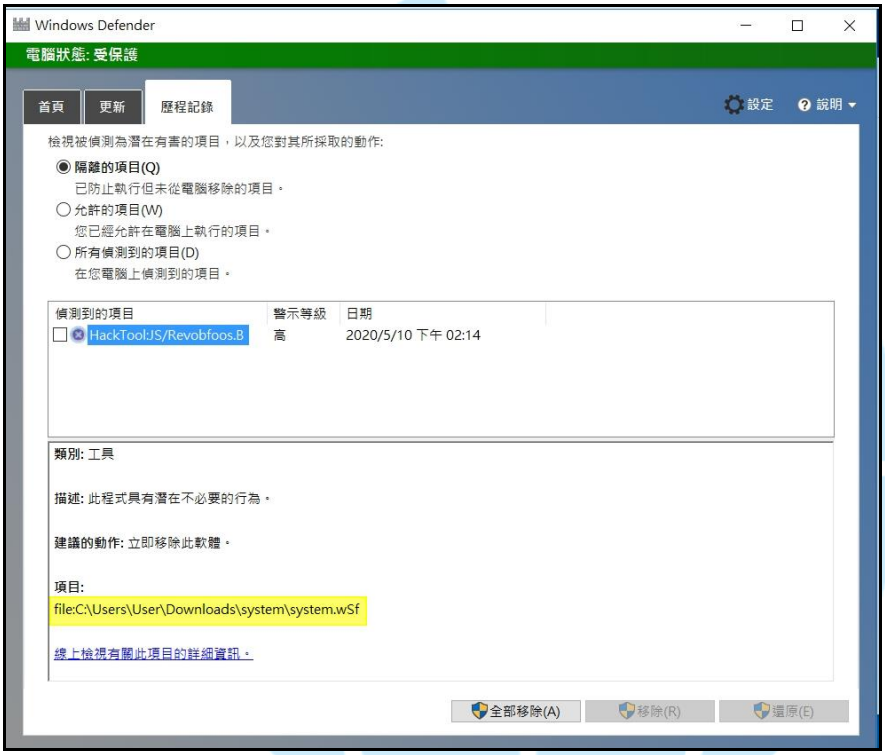






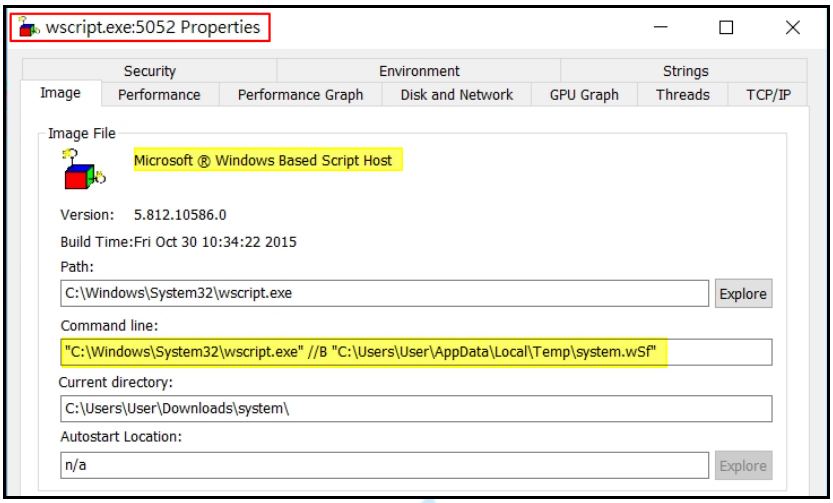
5. 當檢視 system.wSf 的內容時觸發主機內防毒軟體進行掃毒作業，但是並未掃描出該檔案是惡意程式。在此同時防毒軟體也一起完成病毒碼的更新作業，在這之後每當點選 system.wSf 時，防毒軟體會偵測到 system.wSf 的存在，並且隔離它。推測防毒軟體偵測的到它的存在是因為檢視 system.wSf 程式碼與將隱藏系統檔案的設定關閉的關係，因此將該檔案恢復隱藏的狀態並且使用防毒軟體掃描主機，發現防毒軟體偵測不到它的存在。



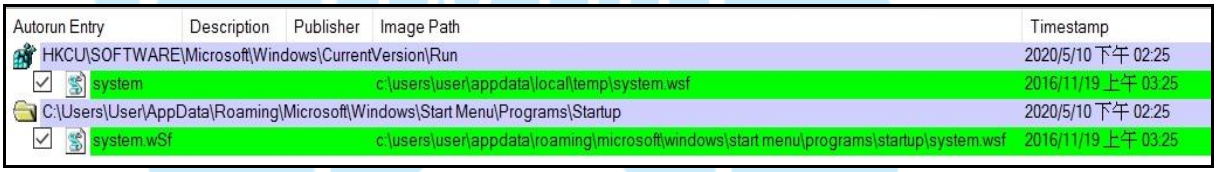


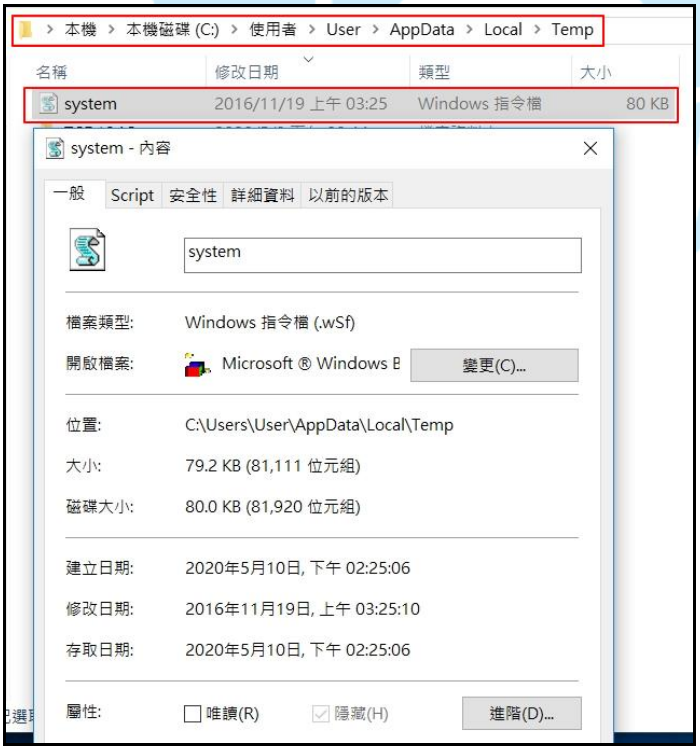
6. 檢視背景程式發現有 wscript.exe 正在執行 system.wSf，而且 system.wSf 來自 C:\Users\User\AppData\Local\Temp 資料夾內的 system.wSf。在 wscript.exe 後面加入「//B 」表示批處理模式，會隱藏使用者提示和指令碼錯誤在命令列中的顯示。

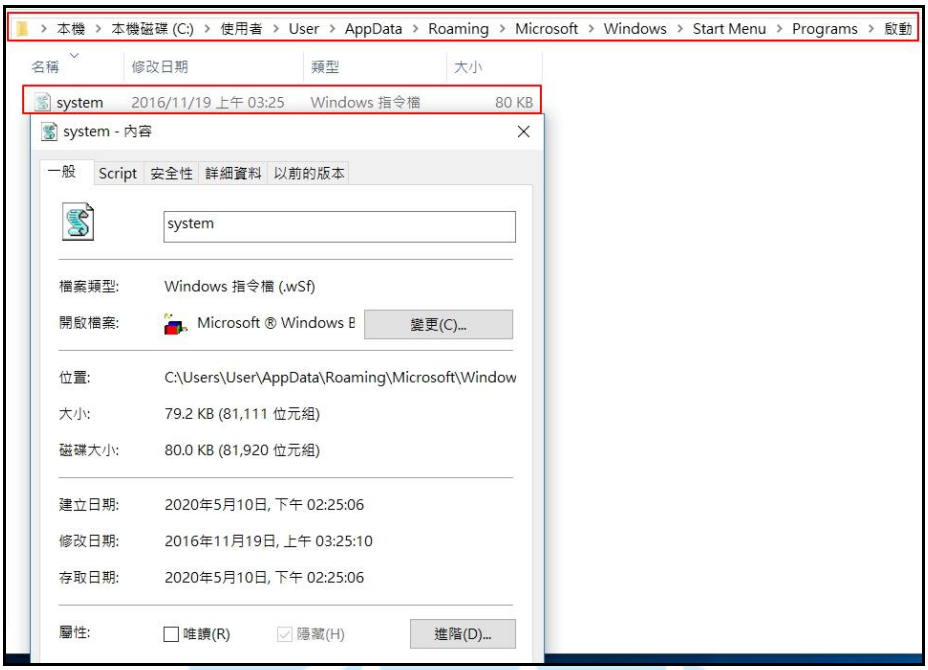
Process	Description	Command	Start Time
WScript.exe (5276)	Microsoft ® Windows Based Script Host	"C:\Windows\System32\WScript.exe" "C:\Users\User\Downloads\system\system.wSf"	2020/5/10 下午 02:25:05
wscript.exe (5052)	Microsoft ® Windows Based Script Host	"C:\Windows\System32\wscript.exe" //B "C:\Users\User\AppData\Local\Temp\system.wSf"	2020/5/10 下午 02:25:06



7. 檢視主機開機狀態的設定，發現 system.wSf 執行後會將自己複製至 C:\users\user\appdata\local\temp 資料夾與 C:\users\user\appdata\roaming\microsoft\windows\start menu\programs\startup 資料夾內，而且因為該檔案為隱藏的系統檔狀態，故不容易被使用者發現它的存在。此外，它也修改註冊檔、設定自己在每次開機後自動執行。

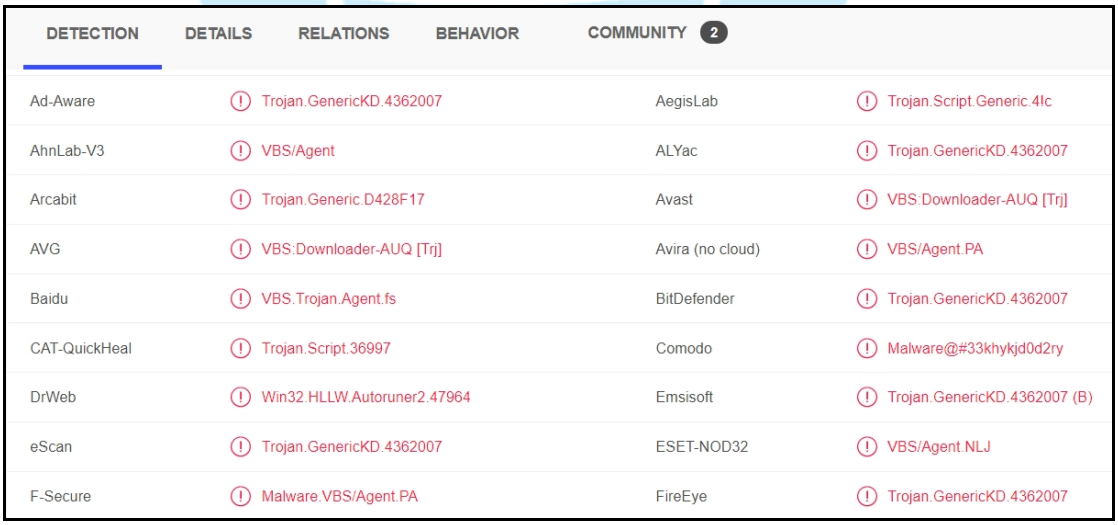






8. System.wSf 經 Virustotal 檢測其惡意比例為 38/58，若它未隱藏則仍有許多防毒軟體無法偵測出它的存在。

從 38 家偵測出它存在的防毒軟體命名得知，它的特性是 VBS Backdoor、Networm、VBS.Downloader、Trojan.Scriprt 與 VBS_AutoRun。



Fortinet	VBS/Agent.NLJIworm	GData	Trojan.GenericKD.4362007
Ikarus	Worm.VBS.Agent	Jiangmin	Trojan.VBS/Agent.a
K7AntiVirus	NetWorm (0051b4ba1)	K7GW	NetWorm (0051b4ba1)
Kaspersky	HEUR:Trojan.Script.Generic	MAX	Malware (ai Score=100)
McAfee	VBS/BackDoor-FAA	McAfee-GW-Edition	VBS/BackDoor-FAA
Microsoft	HackTool:JS/Revobfoos.B	NANO-Antivirus	Trojan.Script.Agent.esqnxn
Qihoo-360	Virus.vbs.qexvmc.1	Sangfor Engine Zero	Malware
Sophos AV	VBS/Dldr-RH	Symantec	Trojan.Gen.MBT
Tencent	Heur:Trojan.Script.LS_Gencirc.7057945.0	TrendMicro	VBS_AUTORUN.AOOA
TrendMicro-HouseCall	VBS_AUTORUN.AOOA	ZoneAlarm by Check Point	HEUR:Trojan.Script.Generic
Dr.Web vxCube	SPREADER MALWARE	Antiy-AVL	Undetected

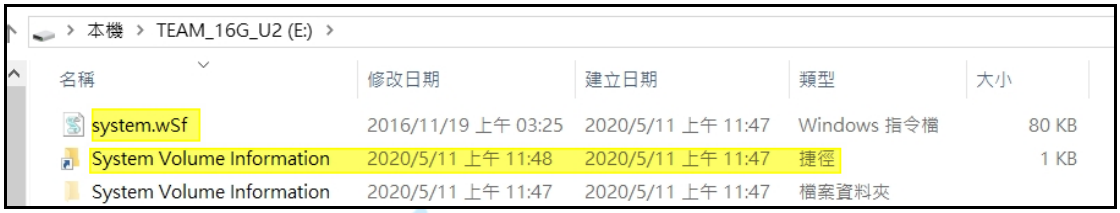
9. 將受測主機重新開機後，在背景程式可以看到 wscript.exe 執行 Temp 資料夾內的 system.wSf 中。

Process	CPU	Private B...	Working Set	Command Line
wscript.exe	< 0.01	5,456 K	16,348 K	"C:\Windows\System32\wscript.exe" //B "C:\Users\User\AppData\Local\Temp\system.wSf"

將含有檔案資料夾的 USB 隨身碟插入主機中，發現隨身碟內自動產生與原來資料夾同名的捷徑檔和一個 system.wSf，而且原來的資料夾皆變成隱藏檔。

因為檢視設定為不隱藏檔案(含系統檔案)，故在上圖仍可以看到原先的資料夾與檔案 system.wSf。若開啟隱藏設定，則使用者僅能看到捷徑檔(如下圖)。

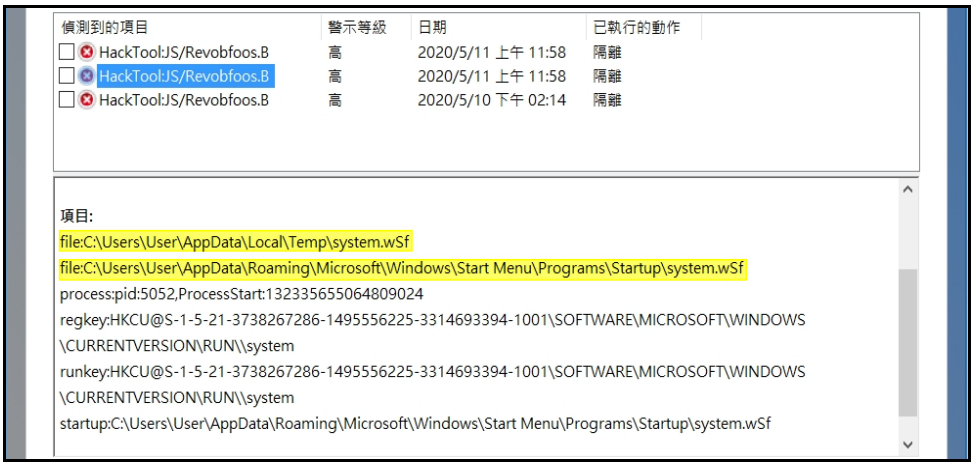
將隨身碟進行格式化，發現原來的資料夾檔案與捷徑檔在格式化後已不存在，但是 system.wSf 與 System Volume Information 資料夾在格式化後還是存在，而且 System Volume Information 還產生一個捷徑檔，推測此行為可能與 wscript.exe 正在執行 system.wSf 有關。



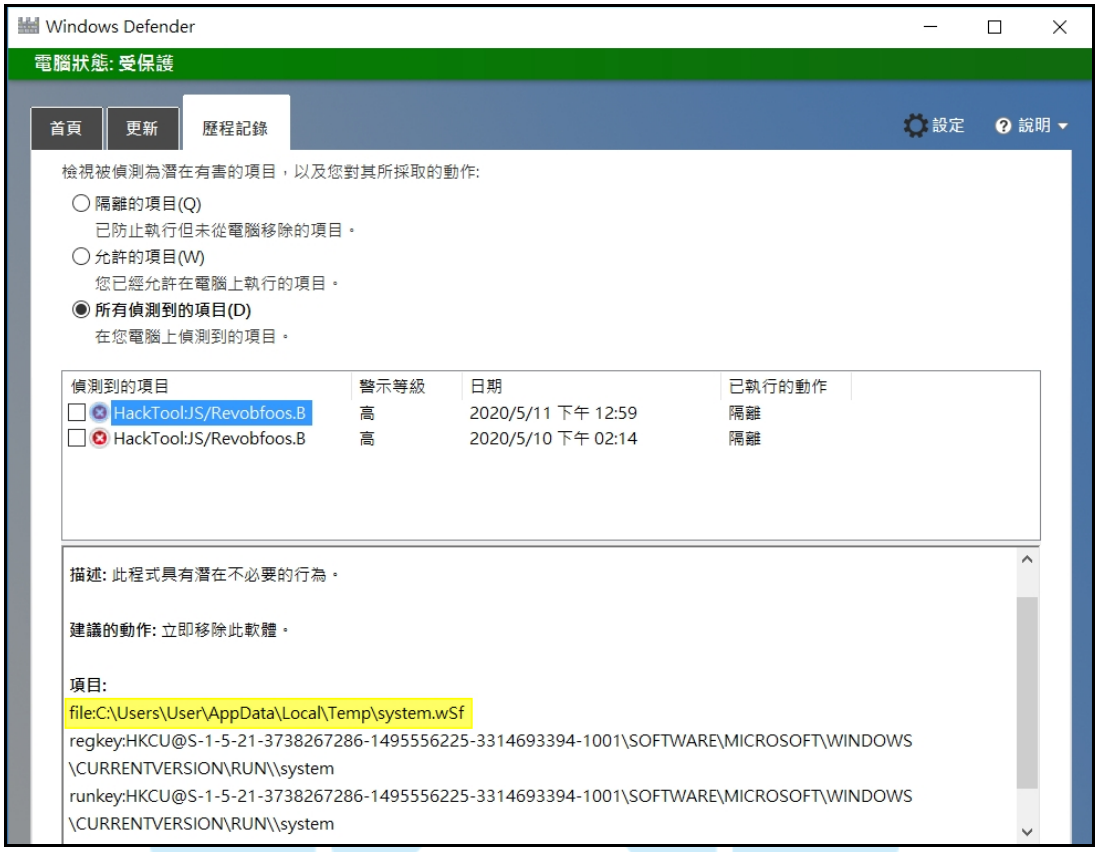
將程序 wscript.exe 暫停，並且將隨身碟格式化，發現 system.wSf 未出現於隨身碟中，而且只剩下 System Volume Information 這一個隱藏的系統資料匣，它是「系統還原」工具用來儲存其資訊與還原點的地方，每個 USB 內都存有此資料匣。

接著若重新執行 wscript.exe，則隨身碟再次感染病毒 system.wSf、將資料夾檔案隱藏並產生捷徑檔。

10. 在 system.wSf 檔案未隱藏的狀況下將防毒軟體開啟，則馬上被偵測到有惡意檔案執行中，而且將存在 C:\Users\User\AppData\Local\Temp 資料夾與 C:\Users\User\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup 資料夾內的 system.wSf 隔離。

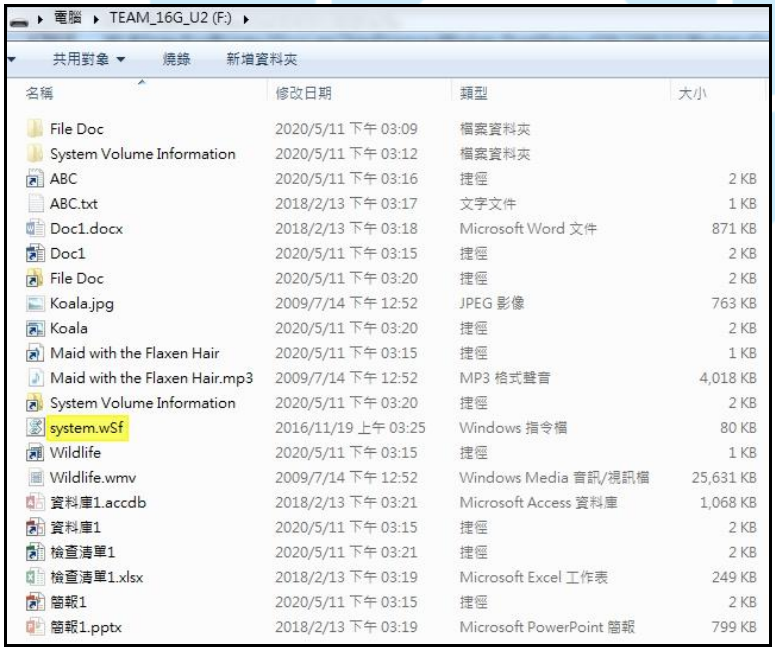


若將 system.wSf 設定為隱藏的狀況下將防毒軟體開啟，則防毒軟體僅偵測到目前 wscript.exe 正在執行的 C:\Users\User\AppData\Local\Temp 資料夾內的 system.wSf。



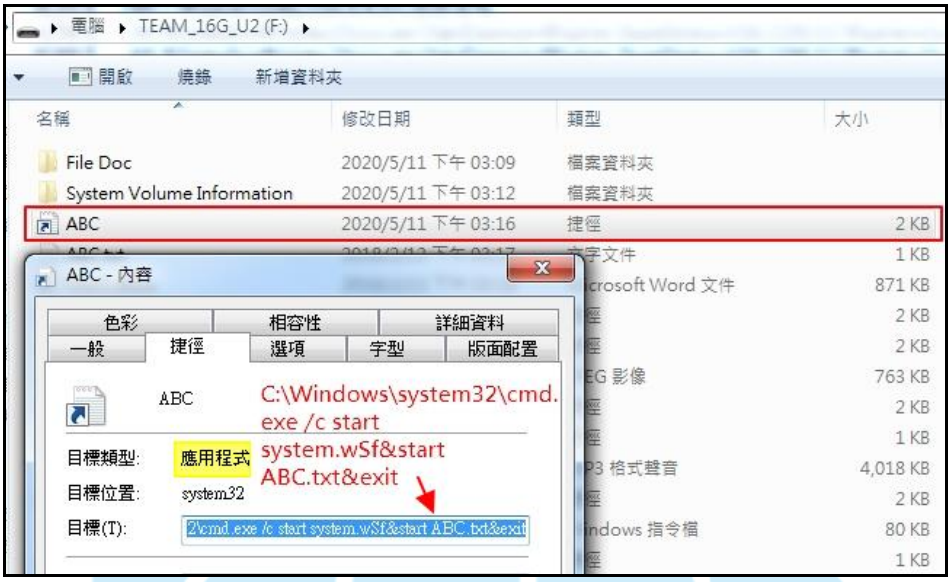
11. 若將 system.wSf 設定為隱藏，並且使用防毒軟體對主機進行「快速掃描或完整掃描」，則防毒軟體可以偵測到 C:\Users\User\AppData\Local\Temp 資料夾與 C:\Users\User\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup 資料夾內的 system.wSf。但是仍無法偵測到原先一開始執行的惡意程式樣本 system.wSf。

12.將含有捷徑檔案而且感染 system.wSf 的 USB 隨身碟插入另一台主機，發現插入後若沒有點選 USB 內的捷徑檔，則該台主機不會感染 system.wSf。若點選任何一個捷徑檔，則該主機會執行 wscript.exe 來執行 system.wSf。

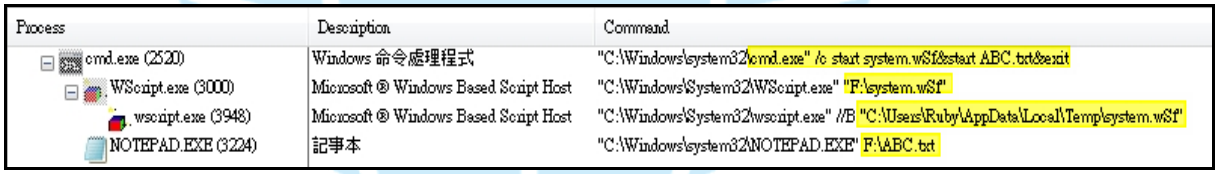


13.檢視 ABC 捷徑檔的內容，發現該檔案的目標類型為應用程式，而且在目標內有一串指令「"C:\windows\system32\cmd.exe" /c start system.wSf&start

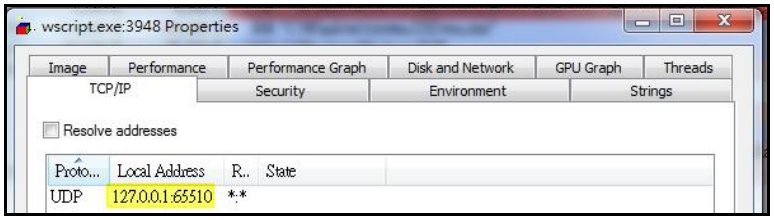
ABC.txt&exit」。當點選該捷徑檔時，系統會執行隨身碟內的 system.wSf 而且也會開啟 ABC.txt 文字檔。查看其他的捷徑檔內容，其內容皆是執行 system.wSf，並且開啟原捷徑檔所對應的檔案。



14. 檢視背景程式的執行紀錄，發現在 ABC 捷徑檔被點選後，cmd.exe 開始呼叫 WScript.exe(3000)來執行 F:\system.wSf，也呼叫 NOTEPAD.EXE(3224)來開啟 F:\ABC.txt。在 WScript.exe(3000)執行 F:\system.wSf 後，它會呼叫 wscript.exe(3948)來執行在 C:\Users\Ruby\AppData\Local\Temp\system.wSf。該檔案是隨身碟內的 system.wSf 執行後，在主機上新增的檔案 system.wSf。



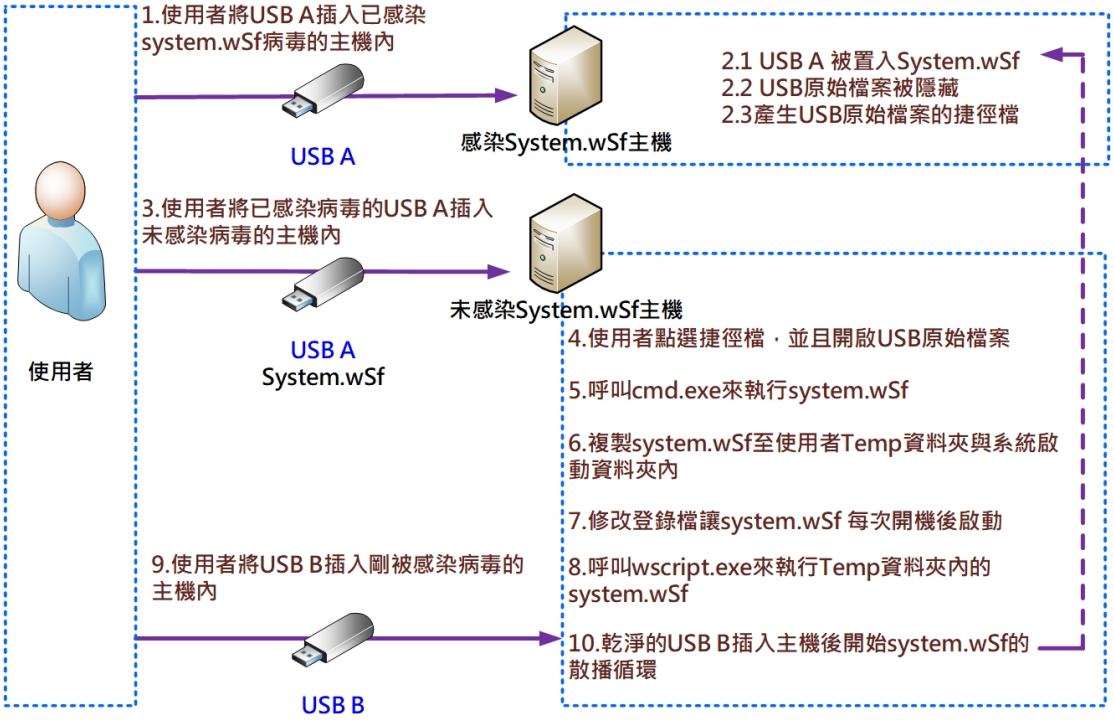
15. 檢視 wscript.exe(3984)的內容，發現該主機會對外開啟 65510 port，提供遠端任意 IP 的 UDP 連線。



16. 查看新感染主機開機後的程式啟動情形，發現與前面受感染主機相同特徵。在新感染的主機上也會在開機後自動執行 system.wSf。

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020/5/11 下午 03:31
system	Microsoft ® Windows Based Script Host	Microsoft Corporation	c:\windows\system32\wscript.exe	2009/7/14 上午 07:42
C:\Users\Ruby\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2020/5/11 下午 03:31
system.wSf			c:\users\ruby\appdata\roaming\microsoft\windows\start menu\programs\startup\system.wsf	2016/11/19 上午 03:25

三、事件攻擊行為示意圖



1. 使用者將 USB A 插入已感染 system.wSf 病毒的主機內。
2. USB A 插入後被執行下列動作:

   2.1 USB A 被置入檔案 System.wSf。

   2.2 USB 原始檔案被隱藏。

   2.3 產生 USB 原始檔案的捷徑檔。
3. 使用者將已感染病毒的 USB A 插入未感染病毒的主機內。
4. 使用者點選 USB A 內的任一捷徑檔，並且開啟該捷徑所對應的 USB 原始檔案。
5. 呼叫 cmd.exe 來執行 system.wSf。
6. 複製 system.wSf 至該主機的使用者 Temp 資料夾與系統啟動資料夾內。

7. 修改登錄檔讓 system.wSf 每次開機後能啟動。
8. 呼叫 wscript.exe 來執行 Temp 資料夾內的 system.wSf。
9. 使用者將 USB B 插入剛被感染病毒的主機內。
10. 乾淨的 USB B 插入主機後開始 system.wSf 的散播循環。

四、總結與建議

1. 惡意程式 system.wSf 偽裝為 Windows 指令檔，當被執行時會複製自己於使用者的 temp 資料夾與主機的系統啟動資料夾內。
2. System.wSf 由於其為系統檔案，而且本身設定為隱藏，不容易讓受害者發現其所在之處。一般防毒軟體雖然開啟偵測模式，但若它沒有使用 wscript.exe 來執行程式，則未必能偵測到它的存在。
3. System.wSf 會對插入主機的隨身碟進行病毒感染，將 system.wSf 複製一份至隨身碟中。它也會將隨身碟內的檔案隱藏起來，並且產生偽裝為路徑檔的應用程式。
4. 當使用者開啟隨身碟時，只看到路徑檔存在。在使用者點選路徑檔後會執行在隨身碟內的 system.wSf，以及開啟路徑檔所對應的實際檔案。透過這個執行 system.wSf 的動作將此病毒感染至新的主機內，而且因為路徑檔有開啟原來對應的檔案，讓使用者不會懷疑該路徑檔會執行惡意程式。
5. 因為 wscript.exe 執行著 system.wSf。若對已插入主機的 USB 隨身碟進行格式化，仍然無法將隨身碟內的 system.wSf 移除，需要將 wscript.exe 暫停或停止後對 USB 隨身碟進行格式化，才能完全將此程式 system.wSf 移除。
6. 由 Virustotal 的檢測結果得知全世界防毒軟體的種類約有五、六十種，目前僅有 38 種防毒軟體可以偵測到 system.wSf 的存在，能被檢測出的比例不高。

7. 一般主機在有最新防毒軟體的防護下，當 wscript.exe 執行 system.wSf 或開機時啟動 system.wSf 時會被防毒軟體偵測到，進而隔離或移除該程式。但對於一開始執行的病毒樣本 system.wSf，因為其為隱藏的系統檔，若沒有任何執行行為，是沒辦法被防毒軟體掃描到它的存在。
8. 對於預防此類病毒感染的防護措施，除了定期更新病毒碼與定期進行掃毒作業外，建議使用者不要將重要檔案存放於隨身碟中，需要做好檔案備份作業。此外，也建議不要隨意點選不明來源的檔案，以免觸發惡意程式。