

關於 USB 病毒的說明及處理程序

2007年10月09日 銳傑科技股份有限公司提供

本專案服務建議書為銳傑科技股份有限公司版權所有, 未經所有權人授權同意,嚴禁任何形式之複製及使用。

目錄

•	USB 病毒感染方式說明	.02
•	避免 USB 外接裝置感染電腦	.03
•	遭受病毒感染之 USB 外接儲存裝置處理方式說明	.04
•	常見的 USB 病毒 (kavo)的手動處理方式 №	· 件

【前言】

銳傑科技資訊安全部門近來持續監控、分析及統計,發現企業遭受威脅感染來源除了從以往透過瀏覽 HTTP 網頁、接收 Email 電子郵件及網路資源分享等感染橫散途徑外,近來發現來自於 USB 外接儲存裝置感染比例持續增加。

此類惡意程式的作者及駭客,利用 USB 外接儲存裝置使用方便,儲存容量大及各企 業均未對此類裝置進行管制之特性,因此利用 USB 外接儲存裝置威脅惡意程式持續 變種,且擴散速度快速。

【USB 外接儲存裝置病毒感染方式說明】

一、 什麼是 USB 外接儲存裝置

- 1. USB 隨身碟,或稱 USB 大姆碟
- 2. 數位相機或是行動電話使用之記憶卡
- 3. USB 外接式硬碟
- 4. MP3 數位多媒體播放器,例如: Apple lpod
- 5. 含有儲存功能或外接記憶卡之行動電話
- 二、 病毒威脅惡意程式如何透過上述裝置進行感染
 - 目前 Windows 作業系統內建自動執行 (Autorun 或 Autoplay)的功能,當 上述裝置連接至系統後,系統會自動尋找 Autorun.inf 檔案,並且自動執 行 Autorun.inf 中所指定執行相關程式之特性。
 - 故惡意程式作者就利用作業系統此特性,將惡意程式存入上述外接儲存 裝置中,並建立自動執行程式(Autorun.inf)。
 - 當系統連接含有惡意程式之外接儲存裝置時,惡意程式即會自動執行, 並感染系統同時將惡意程式及自動執行程式(Autorun.inf)複製至系統中所 有磁碟機。
 - 同時,利用已感染之作業系統或是含有惡意程式之外接儲存裝置,進行 散佈。

【如何避免遭受 USB 外接儲存裝置病毒感染】

- · 、 By Pass 執行自動執行程式(Autorun.inf)
 - 在系統要連接一個 USB 外接儲存裝置時,在裝置要插入電腦時,一直按 著鍵盤「Shift」鍵,直到系統連結此裝置完成後,再放開鍵盤「Shift」 鍵,此時,作業系統將不會執行 autorun.inf 的內容。
 - 此時請用「檔案總管」,用視窗左邊的樹狀結構來瀏灠或開啟外接儲存 裝置中的檔案,就可避免遭受感染;不要用「我的電腦」或是「檔案總 管」中,對磁碟機代號點兩下的方式,瀏灠或開啟外接儲存裝置中的檔 案。

111 研組尿界

二、 關閉系統自動執行 (Autorun 或 Autoplay)的功能

- 1. 透過修改系統登錄機碼,關閉系統自動執行功能
 - (1) 執行 regedit,找到下列二組機值,將 NoDriveTypeAutoRun 的值修改為 0×00000095,並重新開機,即可停用自動執行功能
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Policies\Explorer
 - HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\ Current Version\Policies\Explorer
 - (2) 利用群組原則嵌入式管理單元 (gpedit.msc), 關閉系統自動執行功能
 - 在[本機電腦]->[開始]->[執行]->[在開啟欄中輸入 gpedit.msc]
 - 當出現群組原則編輯器時,針對[本機電腦]->[電腦設定]->
 - [系統管理範本]->[系統],參考下圖

3°本機電腦原則 - 風電脳設定	■ 系統			
 ■ ● 軟體設定 ■ ● Windows 設定 	闡閉自動播放	設定 一 使 用 者 設 定		
□ □ 系統管理範本	顯示內容	 指令碼 		
Windows Components	需求:	一登入 の10世界の第5		
王 🔄 系統	至少需要 Microsoft Windows 2000			
□ 細路	描述:	■ 群組原則		
使用者設定	關閉自動播放功能。	一 遠端協助		
田 ● 軟體設定 □ ● Windows 設定	一旦您將媒體插入磁(光)碟機,自動 播放就會開始讀取內容,如此一來, 安裝程式檔案和音訊媒體上的音樂便 立即啓動。	 ■ 糸純遠原 ● 結果報告 		
王 🦲 系統管理範本		── Windows 檔案保護		
		□ 遠端程序呼叫		
	依照預設, 卸除式磁碟機(例如軟碟 機,但不含 CD-ROM 光碟機)和網路 上磁碟機的自動播放功能是在停用狀 態。	Windows時間服務		
		□ 分散式 COM		
		🚔 將可能不安全的 HTML 說明功能限制於指定的資料夾	尚未設定	
	如果您啓用這項設定,您也能夠停用 CD-ROM 光辉微的自動播放、或停用	資 登入時不要顯示 [管理您的伺服器] 畫面 · · · · · · · · · · · · · · ·	尚未設定	
		周 總小剛俄尹什坦和語 會 啓動闘機事件追蹤器系統狀態資料功能	同不設定 尚未設定	
	所有磷磷锑的自動播放。	🚰 啓用持續的時間戳記	尚未設定	
	這項設定會停用其它類型磁碟機的自動機能力。	新指定 Windows 安装檔案的位置	尚未設定	
	助播放功能。如果磷磷铁的自動播放功能是預設停用的話,您就無法利用	着 指定 Windows Service Pack 女装幅茶位直	向木設定	
	這項設定來啓用該功能。	餐 詳細資訊相對於狀態訊息	尚未設定	
	請注意:這項設定同時出現在[電腦設	会 禁止這些程式從說明中啓動	尚未設定	
	定]和[使用者設定] 資料夾中,如果兩 個地方的設定發生術空,「兩脳設定]	瞬間時自動播放	尚未設定	

點選右邊視窗中[關閉自動播放],將其設定為[已啟用],在停用自動播放在的部份設為[所有磁碟機],並重新開機,即可停用自動執行功能

關閉自動播放 內容	? ×
設定解說	
蘭閉自動播放	
○ 尚未設定(C)	
○ 已啓用(E)	
○ 已停用①	
支援在: 至少需要 Microsoft Windows 2000 上一個設定(P) 下一個設定(N)	
確定 取消 套用	(A.)

【遭受病毒感染之 USB 外接儲存裝置處理方式說明】

- 一、 關閉系統自動執行的功能
- 二、 用啟系統中「顯示隱藏檔」功能
- 三、 若該病毒防毒軟體已可偵測時,請執行全系統掃描,以刪除系統中受感 染的檔案
- 四、 删除 USB 外接裝置中的 autorun.inf 等自動執行程式
- 五、 刪除 USB 外接裝置中的病毒檔案
- 六、 删除系統中病毒所新增之機碼值
- 七、 回復系統 C:\及 D:\等磁碟機開啟程式的設定

【銳傑提供工具說明】

- 一、由於目前此類透過外接裝置感染的威脅,均會修改系統設定,導致系統 無法顯示隱藏檔案及系統 C:\等磁碟機無法正常開啟,需透過修改系統 機碼方式才可復原,以下連結所下載之工具,執行後自動修復無法顯示 隱藏檔案及系統 C:\等磁碟機無法正常開啟之問題。 http://www.eranger.com.tw/soft/fix_usb.exe
- 二、目前透過外接裝置感染的威脅變種迅速,防毒軟體可能無法於第一時間 偵測攔截所有的變種威脅,以下連結所下載之工具,會將病毒檔案刪除 並且把病毒檔案複製一份到C磁碟機 VIRUS 資料夾下,如果此資料下 有新的 USB 變種病毒產生請把此資料夾壓縮加密後寄到 [銳傑科技客戶服務部]信箱 <u>customerservice@eranger.com.tw</u>分析 位置如下:(此工具建議於安全模式下執行才可將病毒有效清除) <u>http://www.eranger.com.tw/soft/remove_usb_virus.exe</u>

【附件】常見的 USB 病毒 (kavo)的手動處理方式

- (1) 先執行 cmd 呼叫「命令執行視窗」【步驟 2~4 請在命令執行視窗裡下指 令】
- 執行 attrib -S -H -R x:\autorun.inf
 執行 attrib -S -H -R x:\ntdelect.com
 執行 attrib -S -H -R c:\windows\system32\kavo*.*
 注意:x代表自己的磁碟機,所有分割的磁碟機都要
- (3) del c:\windows\system32\kavo.exe del c:\windows\system32\kavo0.dll (可能會產生多個檔案 kavo1.dll, kavo2.dll 等等...) del x:\autorun.inf del x:\ntdelect.com 注意: X 代表自己的磁碟機,所有分割的磁碟機都要 注意: 不要砍錯檔! ntdetect 是 winxp 系統檔, ntde『I』ect 才是木 馬!
- (4) 用 attrib x:\autorun.inf 和 attrib x:\ntdelect.com 檢查所有磁碟機是否還有 相同檔案產生
- (5) 執行 regedit
- (6) 找到 [HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Run]裡有一個執行 c:\windows\system32\kavo.exe 的值 ,有的話請刪除
- (7) 找到[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL]裡的一個 值 CheckedValue 把它改成 1
- (8) 如果 kavo*.dll 無法刪除則第7步驟完成後,就先重開機,選擇進入「安 全模式」應該就可以刪除了
- (9) 成功刪除 C:\windows\system32\kavo*.dll 後,再檢查一次第7步驟的值 有沒有改成功
- (10)上述步驟如都有完成則再重開機後試試看能不能「顯示隱藏檔」 (如木馬在的時候,就算選了顯示還是會跳回去)如果可以顯示隱藏檔 就是已成功清除木馬!
- (11) 注意:此時請您點擊看看我的電腦中的C、D 槽,若是出現所有的磁碟 都無法開啟....而是要選擇開啟的程式,請刪除下列位置機碼即可正常 Windows Xp, 2003 server [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersio n\Explorer\MountPoints2] Windows 2000 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersio

n\Explorer\MountPoints]