USB病毒防範與解除

ccjh.kl.edu.tw/modules/tad_book3/html_all.php

USB病毒防範與解除

USB Virus Killer 快速移除USB病毒的小程式。

下載後解壓縮,直接點擊USBVirusKiller.exe即可。

USB_Virus_Killer

解除Helper.vbs等變種的USB病毒的批次檔(壓縮檔)。

Remove_USB_Virus

下載後於解壓縮檔案,於*.bat上點擊滑鼠右鍵,選取「以系統管理員身份執行」,如下圖:



於如下畫面處點擊你所想要執行的選項:



USB病毒防範與解除

3. USB病毒的徵狀

最重要的判斷依據,就是隨身碟(硬碟、記憶卡...),本來的檔案或資料夾全變成「捷徑」。如下圖示例:

當然,這種情形下,檔案根本無法開啟,通常病毒會將自已隱藏起來,如果使用者點擊捷徑,就會將病毒複製到 硬碟並執行,最後整台電腦的C:\下所有的資料夾或檔案可能都變成「捷徑」。

G 、 、 電腦 、 KINGSTON (2)	• 4	, ##	
🐚 HAME - 🔠 MM - 📑 MM -	👼 列印 📼 電子報件 🏀 波線		6
最爱的语言	名稱	修改日期	頭型
	autorun.inf	2012/5/1 下午 04:46	安裝資訊
	DCIM	2012/5/1 下午 04:46	建位
10 地址的建筑	MSMETADATA	2012/5/1 下年 04:46	建位
となる	UNI671C.tmp	2012/5/2 上午 08:19	TMP 檔案
公開	WMDRM	2012/5/1 下午 04:46	連信

USB病毒防範與解除

4. 防範USB病毒-Fortinet Antivirus

Forticlient Antivirus為著名資安公司 - Fortinet所出品的一套免費版的防毒軟體。在Windows Server上也可以安裝。

官方下載點

下載後,於FortiClientOnlineInstaller.exe點擊滑鼠左鍵進行安裝。出現如下畫面,請點擊「是」。

^{使用者帳戶控制} 您是否要允許此 App 變	× 更您的裝置?
FortiClient Online I	nstallation
已驗證的發行者: Fortinet Tech 檔案來源: 此電腦上的硬碟	nologies (Canada) Inc.
顯示更多詳細資料	
是	否

安裝時電腦需要連上網路,安裝程式會下載安裝檔,下載完畢後會進行解壓縮。如下圖。

FortiClient Installer	
Status Downloading image (0%)	Cancel
FortiClient Installer	

在進行安裝主程式前,會對Windows系統進行掃毒的動作。如下圖。

FortiClient Vi	ïrus Cleaner	×
Scanning for virus	ses and malware, this will take a couple of minutes	
Action: Location: Item: Scanned files: Infected files:	scan c:\program files\java\jre1.8.0_144\bin javaws.exe : 2707 Scanned boot blocks: 0 0 Infected boot blocks: 0 Pause Stop	
Status	Virus Infected Item	
< Log file: C:	> XUsers\ccjh\AppData\Local\Temp\FCPreScan\logs\av	

掃毒完畢,會出現如下畫面,請勾選如下圖所示紅色框線處,再點擊Next。

FortiClient Setup - □ ×
Welcome to the FortiClient Setup Wizard
The Setup Wizard will install FortiClient on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Ves, I have read and accept the License Agreement Cancel
接著會出現如下畫面。
😸 FortiClient Setup - 🗆 🗙
Choose Setup Type Choose the setup type that best suits your needs
Security Fabric Agent Endpoint telemetry, host vulnerability scanning and remediation Secure Remote Access SSL and IPsec VPN
Advanced Persistent Threat (APT) Components FortiSandbox detection and quarantine features
Additional Security Features
Back Next Cancel

將圖示上APT與Additional Security Features兩處勾選起來,接著點擊Next。

🖟 FortiClient Setup		-		×
Choose Setup Type Choose the setup type that best suits you	ur needs			
Security Fabric Agent Endpoint telemetry, host vulnerabi	ity scanning and remediat	on		
Advanced Persistent Threa FortiSandbox detection and quarar	t (APT) Components	1		
AntiVirus Web Filtering	Single Sign On			
	Back Nex	t	Canc	el

於Additional Security Features處,勾選Antivirus、Web Filtering與Application Firewall,以對Windows進一步的 防護。

點擊Next後出現如下畫面,要求設定安裝路徑,維持預設值即可。

🖟 FortiClient Setup		-		×
Destination Folder Click Next to install to the default folder of	or click Change to choo	se another.		
Install FortiClient to:				
C:\Program Files\Fortinet\FortiClient\ Change				
	Back	Next	Canc	el

點擊Next後,於如下畫面時點擊Install。

🖟 FortiClient Setup			- 🗆	×
Ready to install FortiClient				
Click Install to begin the installation. installation settings. Click Cancel to	Click Back to revi exit the wizard.	ew or change any	r of your	
	Back	Install	Can	cel
安裝過程如下圖。				
🕞 FortiClient Setup			- 🗆	×
Installing FortiClient				
Please wait while the Setup Wizard in	stalls FortiClient.			
Status:				
	Back	Next	Can	cel

安裝完畢後點擊Finish,如下圖。



安裝完畢後,Windows右下角會出現如下圖示。



掃毒方式-選取要掃描的目錄或磁碟,點擊滑鼠右鍵,如下所示。

	檢視							
本機	▶ 新増磁磷	業區 (C:) →	使用者			~	Ō	搜尋 使
^	名稱		^		修改日期		類型	
	📙 ccjh				2017/0/15	· (1	煤安塔	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	公用				開啟(O)			
					在新視窗開啟(E)			
					釘選到 [快速存取]			
					共用對象(H)			>
				٥	為所選檔創建聰明備份			
					還原酱版(V)			
				3	Scan with FortiClient A	AntiVirus		
					加入至媒體櫃(I)			>
					釘選到開始盘面(P)			
					傳送到(N)			>
					剪下(T)			
					複製(C)			
					建立捷徑(S)			
					刪除(D)			

點擊Scan with FortiClient Antivirus即可進行掃毒。如下畫面。

🦉 FortiClien	t Scan Progress		-	- 🗆 X
			Fo	rtiClient
Scanning for viru	uses and malware			
Action: Location: Item: Scanned files:	Scan files C:\Users\ccjh\AppDa StandaloneUpdater-20 1214	ata\Local\Microsoft\OneDriv 017-8-29.1938.4192.1.odl Scanned boot blocks:	e\logs\Common 0	1010001010 0101011010 010, 10100 0110, 01101 0110, 01101 0110, 01101
Infected files:	0	Infected boot blocks:	0	
[Pause	Stop	Show Details >>	

經實際測試,FortiClinet Antivirus的防護能力不差,而且它主要針對「行為」,如企圖寫入系統的惡意程式,或 企圖呼叫Explorer執行隨身碟中惡意的Script,它可直接檔下不良意圖的動作,但掃毒能力平平,不算太優。綜合 而論,比微軟內建的Defender好很多,加上是免費的,而且安裝完畢後,操作介面會變成繁體中文,相當親民好 上手。特此推薦。

USB病毒防範與解除

5. 防範USB病毒-USB Disk Security

如果有一套程式或軟體,當隨身碟一插入電腦的USB時就能自動掃毒,將有問題的檔案移除,那一定可以省下日 後一支支隨身碟掃毒的麻煩與風險,以下介紹zbshareware這公司所出品的一套免費,專們主動掃除USB病毒的小 程式。經王言俊老師實戰測試,發現可以解掉令人困擾的隨身碟病毒。這個小程式,不但是繁體中文,而且可在 隨身碟病毒進入系統前就先解掉,它可以和其它的防毒軟體和平共存,更重要的,它是免費的。

1. 下載網址: Usb Disk Security

2. 點擊USBGuard6.5.0.0.exe,如下圖,請單擊滑鼠左鍵,點擊「是」。

使用者帳戶控制 ×	
您是否要允許此 App 變更您的裝置?	
🔯 USB Disk Security Setup	
已驗證的發行者: Lanzhou Itanium Software Technology Co., Ltd. 檔案來源: 此電腦上的硬碟	
顯示更多詳細資料	
是否	

以下的畫面,直接單擊滑鼠左鍵,點擊「確定」或「下一步」或「安裝」以進行安裝。

選擇安裝	語言	Х
6	選擇在安裝過程中使用的語言:	
	繁體中文	~
	確定取消	

10 OBD Disk Security 又表達ス	- 🗆 X
選擇目的資料夾 選擇安裝程式安裝 USB Disk Security 的位置。	
安裝程式將會把 USB Disk Security 安裝到下面的資料	诙。
按 [下一步] 繼續,如果您想選擇另一個資料夾,請按 [劉覽]	•
C.Program Files/USB Disk Security	瀏覽 (R)
最少需要 12.7 MB 磁碟空間。	
下一步	(N) > 取消
🐻 USB Disk Security 安裝程式	- 🗆 🗙
網址導航 快速安全的網址導航	
□ 設置Linkzb作為瀏覽器主頁	
預設是勾選的,請單擊滑鼠左鍵取消	
預設是勾選的,請單擊滑鼠左鍵取消 (上一步(B) 下一步	(N) > 取消
預設是勾選的,請軍擊滑鼠左鍵取消 《上一步(B) 下一步 至此畫面時,預設會將Linkzb作為瀏覽器的主頁,請單	 (N) > 取消 型擊滑鼠左鍵取消。
預設是勾選的,請單擊滑鼠左鍵取消 《上一步(B) 下一步 至此畫面時,預設會將Linkzb作為瀏覽器的主頁,請單 ③ USB Disk Security 安裝程式	(10) > 取消 ² 擊滑鼠左鍵取消。 - X
預設是勾選的,請單擊滑鼠左鍵取消 《上一步(B) 下一步 至此畫面時,預設會將Linkzb作為瀏覽器的主頁,請單 び USB Disk Security 安裝程式 選擇財加的工作。	 (M) > 取消 ■擊滑鼠左鍵取消。 - □ ×
預設是勾選的,請單擊滑鼠左鍵取消 《上一步(B) 下一步 至此畫面時,預設會將Linkzb作為瀏覽器的主頁,請單 びUSB Disk Security 安裝程式 選擇要執行的附加工作。 選擇要裝程式在安裝 USB Disk Security 時要執行的附加工作。	 (M) > 取消 型擊滑鼠左鍵取消。 - ○ × ↓ が後按 [下一步]。
承設是勾選的,請單擊滑鼠左鍵取消 《上一步(8) 下一步 至此畫面時,預設會將Linkzb作為瀏覽器的主頁,請單 ② USB Disk Security 安裝程式 選擇野執行的附加工作。 選擇安裝程式在安裝 USB Disk Security 時要執行的附加工作。 附加圖示: ② 建立桌面圖示(0) ② 建立块速散動圖示(0)	 (N) > 取消 ■擊滑鼠左鍵取消。 - × × √ が後按 [下一步]。

<上一步(B) 下一步(N) >

取消



點擊「完成」即完成安裝,同時會啟動USB Disk Security執行程式以常駐於系統中,如下圖所示。



3. USB Disk Security的使用:

其實這個小程式不用什麼設定,可於「設置」處設定密碼,避免因公用電腦不小心被使用者關閉了。

USB Disk Security	-	
	② ^{幫助} 忽的電腦正被保護	🔅 設置
保護狀態	保護狀態 保護您的電廠碼設置 ×	
USB監控	密碼設置 舊密碼:	
USB掃描	新花35: 確認密碼:	
安全網址	語言: Chinese ▼	
數據保護	確定 取消 産品店本:6500 (1)	
	 ✓ 推翻成本: 0.0.00 ⊘ 授權狀態: 全功能版 	
PMAE*E	Zbshareware 3	均持

USB監控:預設可自動將掃描到的隨身碟病毒掃掉。

😲 USB Disk Security		– 🗆 X
	② ^{常助} 您的電腦正被保護	🔅 設置
全 保護狀態	U盤監控 宙時監控防止病毒通過U盤進入您的電腦	
USB監控	威脅	狀態
USB掃描		
安全網址		
● 数嫁保護	☑ 自動刪除威脅	刪除全部
■ 一公	安全打開 安全打開U盤的推薦方式。安全打開讓您可以安全打開U盤而不啟動	丙毒。

USB掃描:可點擊如下方「USB免疫」,不過是否真的有效,不得而知。

	② 您的電腦正被保護	? 幫助	🔅 設置
余護狀態	U盤掃描 掃描您的U盤以發現是否有威脅		, R
USB監控	威脅		狀態
CUSE掃描			
安全網址			
委 數據保護			
〔〕 工具	掃描 停止 刪除		刪除所有
隔離箱	USB免疫 禁止PC和U盤的自動運行功能以防止病毒入侵電腦		
∽人/网↓L ·			
女王納址:			
女王納山 : VSB Disk Security	◎ 您的電腦正被保護	? 幫助	- □ ×
女王納中正: ♥ USB Disk Security	安全網址 可以在訪問任意網址前確定安全,並讓您方便快捷地訪問常用網址	? 幫助 。	- □ ×
女王納中正: ♥ USB Disk Security ↓ CSB Disk Security (保護狀態) ↓ USB監控	您的電腦正被保護 安全網址 可以在訪問任意網址前確定安全,並讓您方便快捷地訪問常用網址	? 幫助	- □ ×
女王納中正: ♥ USB Disk Security ● R護狀態 ● USB監控 ● USB開描	您的電腦正被保護 安全網址 可以在訪問任意網址前確定安全,並讓您方便快捷地訪問常用網址	? 幫助 。	- C X
文王納中止: ♥ USB Disk Security ↓ USB Disk Security ↓ USB監控 ↓ USB監控 ↓ USB開描 ↓ USB掃描	 を全網址 のはないので、 のはないので、 のので、 ので、 のので、 ので、 のので、 ので、 ので、	? 幫助 。	- C X
 ★ 王納中止: ♥ USB Disk Security ● 保護状態 ● USB監控 ● USB掃描 ● 安全網址 ● ● 安全網址 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	 を全額址 の成本部間任意網址前確定安全,並譲您方便快捷地訪問常用網址 が以本訪問任意網址前確定安全,並譲您方便快捷地訪問常用網址 が、 の以本訪問任意網址前確定安全,並譲您方便快捷地訪問常用網址 が、 のののののののでは、 のののののののののののでは、 ののののののののののののののののののののののののののののの	? 幫助	- C ×
 ★ 王納中正: ♥ USB Disk Security ♥ (保護状態) ♥ USB監控 ● USB掃描 ● USB掃描 ● 文全網址 ● 数據保護 ● 工具 	 シントンシントン・シントン・シントン・シントン・シント・シント・シントン・シントン・シント・シント	? 幫助	- C ×

數據保護:可設定USB碟只供讀取或防止未授權的人使用。各位可自己試試看。

_

	② 您的電腦正被保護	? 幫助	🔅 設置
全 保護狀態	數據防洩漏 防止您的數據被其他人竊取		
USB監控	U盤只讀控制 防止未授權人拷貝您的數據到U盤		
O USB掃描	鎖定		
安全網址	U盤控制 防止未授權的人在您的電腦使用U盤		
「上	鎖定		
隔離箱			

工具:可進行硬碟清理、系統修復與設定一開機就啟動的程式列表。

😲 USB Disk Security		_		×
	您的電腦正被保護 ? #	助	🔅 設置	
余 保護狀態	条統工具 恢復惡意修改並可以刪除垃圾文件			
USB監控	硬盤清理 刪除垃圾文件並清理IE緩存文件夾			
USE掃描	修復系統 你可以修復系統以還原被病毒做的惡意修改			
安全網址	自動運行列表			
數據保護	新闻行用 Windows 假义 期间 计程序			
Г р				
隔離箱				

V 050 Disk Security				
	这 您的電腦正被	皮保護	? 幫助	🛟 設置
全 保護狀態	隔離 所有被刪除的不安全文件都得	波加密並保存在隔離箱中		
USB監控	原始 K:\autorun.inf.ren K:\sources\SetupError.exe	隔離 C: \Users \CCJH \AppData \ C: \Users \CCJH \AppData \	Roaming \Zbshareware Lab \USB Roaming \Zbshareware Lab \USB	Guard\quarantin Guard\quarantin
QUSB掃描	1			
安全網址	/			
委 數據保護				
Т	[刷新	還原	清空
隔離 箱				

當USB隨身碟或外接式硬碟插入電腦的USB時,系統會自動掃毒,並於螢幕右下角彈出如此小視窗。



這樣各位就可以點擊安全打開,或逕行從檔案總管、我的電腦中開啟USB碟。

USB病毒防範與解除

6. 随身碟內容變成捷徑的處理

如果隨身碟(含可攜式硬碟)已受病毒感染,檔案或資料夾會變成捷徑,如果點擊該捷徑,會將病毒寫入 Windows系統,則該電腦就會受隨身碟病毒感染,最後感染每一支插入該電腦USB的隨身碟。

如果隨身碟內的病毒已被清除,但檔案或資料夾仍是捷徑,這樣子資料仍然無法被讀取,可循下列方式解決。

以Win10為例,於 翰入命令提示字元,並於其上單擊滑鼠右鍵,選擇以「系統管理員身份」執行,如下所示。

 \sim

	篩選條件 🏏
最佳比對	
● ● ■ ■ ■ ■ ■ ■ ■ ● ● ● ■ ■ ● ● ● 是示字元 ■ ■ ■ ■ ■ ● ● 見示字元	
應用程式≫	
🦧 SoftEther VPN 命 令行实用	工具(vpncmd)
\$	
2	
▶ 町マ従不子儿	
💽 系統管理員: 命令提示字元	

Microsoft Windows [版本 10.0.15063]	
(c) 2017 Microsoft Corporation. 著作權所有,並保留一切權利	
C:\WINDOWS\system32>	

假設USB隨身碟的路徑是i,於提示字元輸入i,再按下Enter。

於i:\>,輸入 attrib -s -r -h * /S /D 將被隨身碟病毒隱藏的檔案與資料夾回復。

切記,資料回復後,將隨身碟中所有的捷徑刪除。