Process Explorer エ具應用

## Process Explorer 工具應用

# 開啟方法與下載點: <u>https://docs.microsoft.com/en-</u> <u>us/sysinternals/downloads/process-explorer</u> 目前最新版本「Process Explorer v16.32」

經驗分享 —

#### □ Process 狀態與種類

#### □ 檢查是否為惡意程序

#### □ 驗證程序簽名檔

□ 找出電腦中的惡意程序



	此开生的	百俊,伊	用系統官	理者身份	執行
<ul> <li>Ⅰ</li> <li>□</li> <li>□</li></ul>	管理 應用程式工具	ProcessExplorer			□ × ∩
★ □ □ ↓ 剪下 釘攫到[ 複製 貼上 快速存取]	▲ 道 移至 複製到 40-4	₩ 重新命名	● 新増項目・ 新増 資料夾	<ul> <li>✓</li> <li>✓</li></ul>	全選 計 全選 計 全部不選 ○ 反向選擇 ○ 次回
<del>万和夜</del> ← → × ↑	1	⊣ ⊑ /≊ plorer	ت بر الا	提尋 ProcessExplo	rer p
▲ 快速存取 ■ 桌面 ● 下載	a.txt cexp.chm		修改日期 2019/5/5 上午 11 2019/6/28 下午 0		大小 8 KB 71 KB
<ul> <li>資 文件</li> <li>☆ pro</li> <li>☆ pro</li> <li>☆ a pro</li> <li>☆</li></ul>	cexp.exe cexp64.exe	開啟(O) ● 以系統管理員 疑難排解相容	身分執行(A) 性(Y)		2,761 KB 1,467 KB

下載後啟動-



#### $\Box$ Options $\rightarrow$ Font



基本設定

5





#### □ View → Select Columns

Process Explorer -	əy sinternals: www.sysi		
le Option Viev	Process Find Users Help		
	system Information	Ctrl+I	
	Show Process Tree	Ctrl+T	Des
System	Show Column Heatmaps		
🗾 Interru	Scroll to New Processes		Harc
smss.e	Show Unnamed Handles and Mappings		Win ₩⊨
wininit.e	Show Processes From All Users		Win
	Opacity	•	服养 Win
N N	Show Lower Pane	Ctrl+L	WM
T V	Lower Pane View	+	WM
	Refresh Now	F5	Win
	Update Speed	+	Win
	Organize Column Sets		Win 占定
	Save Column Set		Win
	Load Column Set		工¶
			Goc
	Select Columns		Goc
svchost.	exe < 0 7,164 K 13,144	K 296	Win

#### Verfied Singer

Image Path

□ 勾選下列項目

#### Virus Total



行程類型與顏色-

# □ Options→Color Selection □ 紫色 Packed Images: 表示這個 process 有 特別的被加密處理過。 □ 通常正常的 process 很少會這樣做。病毒的 可能性就很大。 □ Process 的啟動與結束:綠色與紅色。 □ 手手具工具有個常時的 process 就的動象。

哪些Process 啟動、加密、背景服務執行?

□ 看看是不是有經常性的 process 被啟動。或 是莫名的被停止。

- Service 粉紅色: Services 因為一開啟就會 自動的在背景執行。所以可以知道系統有哪 些背景服務與 process 的關係。
- 这藍色行程是由啟動Process Explorer的同一帳戶運行的行程



#### 找出流氓軟體位置並停用

□右下角的彈跳視窗,我們想知道是什麼軟體的彈 跳視窗以及他的目標位置在哪裡

•使用技巧 ——

□點擊圖中像是「靶子」圖示(Find Windows Process),拖動至右下角彈跳視窗

💸 Process Explorer - Sysinternals	: www.sysii	nternals.com			nistrator)	
File Options View Process	Find Ha	andle Users	Help			
Process	CPU	Pri Find Wind	low's Process	(drag over v	window)	Company Name
💶 svchost.exe		4,436 K	2,792 K	1896 Win	idows Services	Microsoft Corporati
svchost.exe 🖶 spoolsv.exe 🕞 spoolsv.exe	0.14	1,812 K 11,272 K 2,084 K	3,188 K 13,836 K 3,376 K	2140 Win 2292 多二 2332 Win	ndows Services 工緩衝處理器子 ndows Services	Microsoft Corporati Microsoft Corporati Microsoft Corporati
					●「日」 <sup>●</sup> <sup>●</sup> <sup>●</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>■</sup> <sup>→</sup>	- C × へ 使用小重 彩・家 3D 遠照
					<ul> <li>の共 Goog</li> <li>自動凍入</li> <li>受 安全放置</li> </ul>	∽
			擾人的廣	告視窗	<ul> <li>● 陽和權和安全性</li> <li>● 外額</li> <li>Q、 搜尋引擎</li> </ul>	網站 使
					(半)	

#### 檢視整體電腦的效能

View > System information (Ctrl + I)



- 使用技巧 ——

## 將特定Process 當下的狀態快照事後分析

□ 利用 "Create Dump" 的功能,將特定 process 當下的狀態儲存

□ 產生的 Dump 可以用 windbg or Diagnosis Tool 事後分析(windbg)

https://docs.microsoft.com/zh-tw/windows-

hardware/drivers/debugger/debugger-download-tools

	1000 C			
🗆 🐂 explorer.exe	0.09	128,304 K	162,952 K 5468 Windows 檔筆	案總管 Microsoft Corporati
$\bigoplus$ Security Health Systra		1,768 K	4,484 K 8412 Windows Sec	urity no Microsoft Corporati
wmtoolsd.exe	0.03	4,064	Window	Core VMware, Inc.
🗢 OneDrive.exe	- Server alle	27,184	THISON	rive Microsoft Corporati
💆 SSScheduler.exe	Senders	2,740	Set Affinity	7 Sca McAfee, Inc.
🗆 🥃 iexplore.exe	0.02	38,464	Cat Drianity	r Microsoft Corporati
🥃 iexplore.exe	< 0	102,512	Set Phoney	r Microsoft Corporati
🖃  iexplore.exe	0.01	46,368	Kill Process Del	r Microsoft Corporati
🚌 splwow64.exe		6,788		for a Microsoft Corporati
🥭 iexplore.exe	< 0	68,556	Kill Process Tree Shift+Del	r Microsoft Corporati
EXCEL.EXE	< 0	68,488	Restart	Microsoft Corporati
POWERPNT.EXE		275,484	Suggest	Point Microsoft Corporati
🖽 🌍 chrome.exe	0.42	178,448	Suspend	Google LLC
🕎 WINWORD.EXE	0.03	210,500	Create Dump	Create Minidump
🖃 🔤 cmd.exe		2,852	oregie partip	
🔤 conhost.exe		11,404	Check VirusTotal	Create Full Dump
🗆 🛃 powershell_ise.exe		112,728		- Shell Microsoft Corporati
🔤 conhost.exe		9,288	Properties	幾 Microsoft Corporati
눩 mmc.exe	0.01	57,804	Search Online Ctrl+M	geme Microsoft Corporati
🚳 msnaint exe	Georgen)	42 196	Currin Currin	Microsoft Corporati

13

使用技巧

#### Process 是不是有偷偷往外連

	N.		
Image	Performance	Performance Graph	n Threads
TCP/IP	Security	Environment	Strings
<u>R</u> esolve addre	esses		
Protocol 🔺	Local Address	Remote Address	State
TCP	127.0.0.1:1051	127.0.0.1:1025	ESTABLISHED
UDP	127.0.0.1:1043		
<		101	
	Thread stac	k at time port was opene	ed Stack

- 使用技巧 ——

1Δ

### 檢查是否為已知病毒?

 $\rightarrow$ 

 $\leftarrow$ 

 $\odot$ 

https://www.virustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489e394
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489e394
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489e394
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489e394
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489eg4
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489eg4
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd489eg4
 https://www.wirustotal.com/gui/file/d63fa94ef4dcc7d988b97605c2deaddc38c58beb63bd48
 https://www.wirustota

使用技巧 ——

			vmtoolsd	.exe:8476 Pro	operties		<u>200</u> 7	
d63fa94ef4	dcc7d988b9	7605c2deaddc38c58beb63l	GPU Graph Image	Threads Performance	TCP/IP Per	Security formance Gra	Environme ph Disk	nt Strings and Network
0	🕢 No en	gines detected this file	- Image File Version: Build Tim	VMware Too (Verified) VM 10.0.0.500- e: Thu Aug 20	ols Core Se 4ware, Inc 16 18:19:43 :	rvice 2015		
/ 70	1006 04 64		Path: C:\Prog	ram Files\VMwa	re\VMware	Tools\vmtoo	lsd.exe	Explore
	d63ta94et4	acc/assps/605c2deaddc38c58bet	Comman	d line:		N		
	vmtoolsd.exe	3	"C:\Prog	gram Files\VMw	are\VMwar	e Tools\vmto	olsd.exe <sup>*</sup> -n vi	nusr
	6 Abite	assambly availage assay	Current	lirectory:				
Community	040415	assembly overlay peexe s	C:\Wind	ows\System32	1			
Score			Autostar	t Location:			-	
00010			HKLM	OF I WARE Mich	osoft\Wind	lows\Current	/ersion \Run \Vi	Explore
			Parent:	explorer.exe(	5468)			Verify
DETECTION	DETAILS	COMMUNITY 1	User:	DESKTOP-KES	T4T0\kai_j	2		
DETECTION	DETAILS	COMMONITY	Started:	上午 12:43:5:	1 2019/8/	16 Image: 6	i4-bit	ing to Front
			Comment:				ł	gll Process
			VirusTotal	0/701		S	bmit	
Acronis		Undetected	Data Even	ution Prevention	n (DED) St	atus: Enabled	(nermanent)	
			Address Sr	aco Load Dapo		Rottom	(permanency	
Accial ab		Undetected	Control Elo	w Guardy	iomizauoff;	Disable	ор 1	
AegisLab		Undetected	Enterprice	Context:		N/A		
			Enterprise	CONCAG		0/6		
							<u>O</u> K	Cancel

#### 驗證是否具有簽名檔

ru alapii	Threads	TCP/IP	Security	Environr	ment	Strings
Image	Performance	Perfor	mance Grap	h D	sk and Ne	twork
Imaga Fila	5					
	VMware Tools	s Core Servi	ce			
VIII	(Verified) VM	ware, Inc.				
Version:	10.0.0.50046	5				
Build Time	e: Thu Aug 20 1	8:19:43 201	15	•		
Path:						-
C:\Prog	am Files\VMwar	e\VMware T	ools\vmtools	d.exe	Exp	lore
Comman	d line:					
"C:\Prog	ram Files\VMwa	re\VMware 1	Tools \vmtoo	sd.exe <sup>*</sup> -n	vmusr	1.
Current	lirectory:					
C:\Wind	ows\System32\					
Autostar	t Location:					
HKLM\S(	DFTWARE\Micro	soft\Window	/s\CurrentVe	ersion∖Run	\VM E <u>x</u> p	lore
Parent:	explorer.exe(54	468)		1		
C GREAT COLUMN	and an and the second second	and the second second		-	Verity	0
User:	DESKTOP-KEST	4T0\kai_je				
User: Started:	DESKTOP-KEST	4T0\kai_je 2019/8/16	Image: 64	1-bit	Bring to F	ront
User: Started:	DESKTOP-KEST 上午 12:43:51	4T0\kai_je 2019/8/16	Image: 64	H-bit	Bring to F	ront
User: Started: Comment:	DESKTOP-KEST- 上午 12:43:51	4T0\kai_je 2019/8/16	Image: 64	H-bit	Ering to F Kill Proce	ront
User: Started: Comment: VirusTotal;	DESKTOP-KEST 上午 12:43:51	4T0\kai_je 2019/8/16	Image: 64	H-bit	<u>Bring</u> to F Kill Proce	ess
User: Started: Comment: VirusTotal: Data Execu	DESKTOP-KEST 上午 12:43:51	4T0 kai_je 2019/8/16 (DEP) Statu	Image: 64	Hbit mit /permanen	<u>Bring</u> to F Kill Proce	ess
User: Started: Comment: VirusTotal: Data Execu Address Sp	DESKTOP-KEST 上午 12:43:51	4T0 kai_je 2019/8/16 (DEP) Statu mization:	Image: 64	H-bit mit (permanen	<u>B</u> ring to F Kill Proce t)	ess
User: Started: Comment: VirusTotal: Data Execu Address Sp Control Flo	DESKTOP-KEST 上午 12:43:51	4T0 kai_je 2019/8/16 (DEP) Statu mization:	Image: 64	1-bit mit (permanen	<u>B</u> ring to F Kill Proce t)	ess
User: Started: Comment: VirusTotal: Data Execu Address Sp Control Flo Enterprise	DESKTOP-KEST 上午 12:43:51 ution Prevention pace Load Rando w Guard: Context:	4T0 kai_je 2019/8/16 (DEP) Statu mization:	Image: 64 Sub s: Enabled Bottom-U Disabled N/A	1-bit mit (permanen	<u>B</u> ring to F Kill Proce	ess
User: Started: Comment: VirusTotal: Data Execu Address Sp Control Flo Enterprise	DESKTOP-KEST 上午 12:43:51 ution Prevention bace Load Rando w Guard: Context:	4T0 kai_je 2019/8/16 (DEP) Statu mization:	Image: 64 Sub s: Enabled ( Bottom-U Disabled N/A	1-bit mit (permanen	<u>B</u> ring to F Kill Proce	ess

- 使用技巧 ——

## 取代/取消 預設的工作管理員(2)





#### □ Options → Verify Image Signatures

Proce	ess Explorer - Sysinternals: www.sysint							2.	
e Op	otions View Process Find Users Run At Logon	s Help							
oc 🗸	Verify Image Signatures	, 2К	Working 4 K	PID D 3852	Description	Company Name	Session Path 0[連結到条	Verified Sig	VirusTotal
	Always On Top Replace Task Manager	р К В К 2 К	23,992 K 160 K 8 K	120 4 0			0 [連結到系 0	200 - 101 - 10 - 00	0.51
	Hide When Minimized Allow Only One Instance	В К В К Д К	45,640 K 4,408 K 9,652 K	5528 3732 64 5564 AI	l-bit Synaptics Poin MD External Event	Synaptics Incorpor . AMD	0 C:\Program F 0 C:\Program F 1 C:\Windows\.	(Venfied) V (Verified) Sy (Verified) Mi	<u>0/71</u> 0/71 0/72
~	Confirm Kill	2 K 4 K 6 K	5,848 K 119,212 K 16 300 K	1568 Al 3956 Ar 123 Ar	MD External Event ntimalware Service pple Push	. AMD Microsoft Corporati Apple Inc	0 C:\Windows\. 0 C:\ProgramD 1 C:\Program F	(Verified) Mi (Verified) Mi (Verified) Ap	0/70 0/70 0/58
1 10 1 10 1	Tray Icons Configure Symbols	) 0 K	8,080 K 6,932 K	3912 At 3472 Bo	theros Coex Servic onjour Service	Atheros Apple Inc.	0 C:\Program F 0 C:\Program F	(主體中目 (Verified) Ap	1/65 0/70
	Configure Colors Difference Highlight Duration	9 K 8 K 8 K	4,352 K 4,332 K 9,420 K	127 Ca 131 Ca 5180 C(	atalyst Control Cent atalyst Control Cent OM Surrogate	Advanced Micro D Advanced Micro D Microsoft Corporati	1 C:\Program F 1 C:\Program F 0 C:\Windows\.	(Verified) Ad (Verified) Ad (Verified) Mi	0/69 0/70 0/67

- 使用技巧 ——

### 檢查是否為惡意程序(所有行程)

#### □ Options $\rightarrow$ VirusTotal.com $\rightarrow$ Check VirusTotal.com

cess Explorer - Sysinternals: www.				
Options View Process Find User	s Help			
Run At Logon			A A A A	
Verify Image Signatures	B Working PID Description	Company Name	Session Path Ver	ified Sig <mark></mark> VirusTot
VirusTotal.com	> 🧹 Check VirusTotal.com			
Always On Top	Submit Unknown Executables		0	
Replace Task Manager	D K 45,580 K 5528		0 C:\Program F (Ver	ified) V 0/71
Hide When Minimized	B K 4,408 K 3732 64-bit Synaptics Po	oin Synaptics Incorpor	0 C:\Program F (Ver	ified) Sy 0/71
Allow Only One Instance	D K 9,652 K 5564 AMD External Eve	ent AMD	1 C:\Windows\ (Ver	ified) Mi <u>0/72</u>
Confirm Kill	2 K 5,848 K 1568 AMD External Eve	ent AMD	0 C:\Windows\ (Ver	ified) Mi <mark> <u>0/70</u></mark>
	5 K 118,648 K 3956 Antimalware Servi	ce Microsoft Corporati	0 C:\ProgramD (Ver	ified) Mi <u>0/70</u>
Tray Icons	b K 16,300 K 123 Apple Push	Apple Inc.	1 C:\Program F (Ver	Ified) Ar <u>0/58</u>
	B K 8,052 K 3912 Atheros Coex Serv	ic Atheros	0 C:\Program F (主責	還甲目 1/05
Configure Symbols	4 K 0,912 K 34 /2 Bonjour Service	Apple Inc.	UC:\Program F (Ver	(fied) Ap $0/70$
Carling Calan	UK 9,776 K 127 Catalyst Control C	ent Advanced Micro D	I C:\rrogram F (Ver	inea) Ad <u>0/09</u>

2

- 使用技巧 ——

21

## 找出可疑程序(2)

□選用其他欄位項目
 □UserName
 □Session

S

#### □View →Select Columns

Process Network	Pro	ocess Disk	Pro	cess Memory
Process GPU Ha	ndle	DLL	.NET	Status Bar
Process Image	Proce	ess Performa	ince	Process I/O
Select the columns that Process Explorer.	will appe	ar on the Proc	ess view o	f
Process Name		Window	Title	
PID (Process Identif	ier)	Window	Status	
User Name	1	Session	2	
✓ Description		Comman	d Line	
🗹 Company Name		Commen	t	
Verified Signer		Autostari	Location	
Version		Virus Tota	al	
🗹 Image Path		DEP Sta	tus	
Image Type (64 vs 3	2-bit)	Integrity	Level	
Package Name		🗌 Virtualize	d	
DPI Awareness		ASLR E	nabled	
Protection		UI Acces	s	
Control Flow Guard		Enterpris	e Context	

出田井丁







#### Process Explorer 工具應用 —

- □ 請先再建立一個系統「還原點」或快照
- □ 請在虛擬機主練習執行「電腦病毒」,並觀察下列資訊:
  - □ USB隨身碟中是否產生相關的病毒程式
  - □ 嘗試刪除USB隨身碟中的「惡意程式」後,有何變化
- □請利用「還原點」/快照還原電腦,再嘗試刪除USB隨身碟中 的「惡意程式」,是否會成功
- □ 成功刪除惡意程式後,還原被隱藏的檔案(解除反白)
- □ 測試再接入USB時,是否還被寫入惡意程式

### 捷徑病毒中毒症狀

#### Process Explorer 工具應用 \_

🔾 💭 🚽 🕨 電腦病毒 🕨 電腦病毒		
組合管理 ▼ 加入至媒體櫃 ▼ 共用對象 ▼ 新増資料夾		
	修改日期	<ul> <li>★小</li> <li>HP-M400印表表-驅動程式 - 内容</li> <li>●彩</li> <li>相容性</li> <li>安全性</li> <li>詳細資料</li> <li>以前的版本</li> <li>一般</li> <li>提徑</li> <li>選項</li> <li>字型</li> <li>版面配置</li> <li>HP-M400印表表-驅動程式</li> <li>目標類型: 應用程式</li> <li>目標(T): system32/cmd.exe /c start Rund1132.js&amp;start explor</li> </ul>
<ul> <li>網路</li> <li>2.會在開機起動項的註冊表 建立一個OBAJQA1XOB的機碼 開機時會啟動位在暫存資料 夾的該腳本</li> </ul>		開始位置③: 快速鍵④: 無 執行(R): 最小化 ▼ 註解(0):
資料參考網址:	C:\Win Rundll &exit	開設幅素位置(P) 愛更圖示(C) 運踏(D) ndows\system32\cmd.exe /c start 132. js&start explorer HP-M400印表表-驅動移 確定 取消 套用(A)

https://gist.github.com/poynt2005/165abc6cdf8d0d1fb9b6c3c98517f2a4

## **捷徑病毒中毒症狀(2)** Process Explorer 工具應用 -

- □ 在USB隨身碟中產生病毒捷徑、隱藏原來的資料與產生 rund1132.js病毒檔
- □ 在登錄表HKEY\_CURRENT\_USER註冊一個vjw0rm的機碼
- □ 會在「開機起動項」的註冊表建立一個OBAJQA1X0B的機碼
   □ 開機時會啟動位在暫存資料夾的該腳本
- □建立排程(每30分鐘執一次)
- □ 讓系統無法顯示隱藏檔
- □ 點選檔案捷徑後,就會感染電腦病毒

#### 解決無法顯示隱藏檔問題





電腦

\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ Advanced\Folder\Hidden\SHOWALL

解決無法取消隱藏問題(2) Process Explorer -

- dir/ah dir/as
- attrib -s -h e:\file 强制解除檔案隱藏指令
- attrib +s +h e:\file 强制進行檔案隱藏指令(GUI)介面會看到 反白的

<ul> <li>× 我的康美</li> <li>▶ 下載</li> <li>▶ System Volume Information</li> <li>▶ test</li> <li>● 最近的位置</li> <li>● 提徑病毒中毒症狀.png</li> <li>● 建徑病毒中毒症狀.png</li> <li>● 建徑病毒-毒症狀.png</li> <li>● 建徑病毒-指令執行方式.txt</li> <li>● 提徑病毒-指令執行方式.txt</li> </ul>	建徑病毒中毒症狀.png       檔案類型:     PNG 影像 (.png)       開設檔案:	變更(C)
<ul> <li>●) 盲葉</li> <li>● 提出/N ● In &lt; + (1) / 2 + (1)</li> <li>● 提出/N ● In &lt; + (1) / 2 + (1)</li> <li>● 電腦病毒.rar</li> <li>● 電腦病毒.rar</li> <li>● 電腦病毒.rar</li> <li>● 電腦病毒.rar</li> <li>● 電腦病毒.rar</li> <li>● 電腦病毒.rar</li> </ul>	位置: E:\ 大小: 86.6 KB (88,761 位元組) 磁碟大小: 88.0 KB (90,112 位元組) 建立日期: 2020年7月3日,下午 10:27:11 修改日期: 2020年7月3日,下午 03:02:42 存取日期: 2020年7月3日,下午 10:27:11 屬性: ■唯讀(R) ☑隱藏(H)	進階(D)

## 解決無法取消隱藏問題(3) Process Explorer -

attrib -s -h e:\file 强制解除檔案隱藏指令 attrib +s +h e:\file 强制進行檔案隱藏指令(GUI)介面會看到

○ ● ■ ● 電腦 ▶ 抽取式磁碟(E:) ▶		<ul> <li>✓ 49 授募抽取式磁碟(E:)</li> </ul>
組合管理 ▼ 🔄 預覽 ▼ 列印 新城	資料夾	C:\Windows\system32\cmd.exe
<ul> <li>★ 我的最愛</li> <li>▲ System Volum</li> <li>■ 桌面</li> <li>● 最近的位置</li> <li>● 提徑病毒中毒</li> <li>● 建徑病毒-指令</li> <li>● 建徑病毒-指令</li> <li>● 建徑病毒-指令</li> <li>● 建徑病毒-指令</li> <li>● 建徑病毒-指令</li> </ul>	<ul> <li>▶ 捷徑病毒中毒症狀.png - 內容</li> <li>→般 安全性 詳細資料</li> <li>▶ 捷徑病毒中毒症狀.png</li> <li>檔案類型: PNG 影像 (.png)</li> <li>開啟檔案: 函 Windows 相戶檢視器</li> <li>位置: E.\</li> </ul>	<ul> <li>磁碟區 E 中的磁碟沒有標籤。</li> <li>磁碟區序號: 7692-C3A8</li> <li>E:\的目錄</li> <li>2020/07/03 下午 10:57 188,830 Rundll32.rar</li> <li>2020/07/03 下午 10:57 188,830 Rundll32.rar</li> <li>2020/07/03 下午 10:57 2020/07/03 下午 10:54 732 捷徑病毒中毒症狀.pn</li> <li>2020/07/03 下午 10:54 738 提徑病毒-指令執行方</li> <li>2020/07/03 下午 10:54 1,512 電腦病毒.rar.lnk</li> <li>4 個檔案 191,812 位元組</li> <li>1 個目錄 7,671,369,728 位元組可用</li> </ul>
■ 代記 = 置 圖片	大小: 86.6 KB (88,761 位元組) 磁碟大小: 88.0 KB (90,112 位元組)	E: \>attrib A E: \Rund1132.rar
📜 電腦	建立日期: 2020年7月3日,下午10:27:3	SH E:\捷徑病毒中毒症狀.png A E:\捷徑病毒中毒症狀.png.lnk
🏭 本機磁碟 (C:)	修改日期: 2020年7月3日,下午03:02:4	42 SH E:\提徑病毒-指令執行方式.txt
👝 抽取式磁碟 (E:)	存取日期: 2020年7月3日,下午10:27:	11 E:\提怪病毒-指受執行力式.txt.Ink SH E:\電腦病毒.rar
System Volum test	屬性:	A E:\電腦病毒.rar.lnk 進階@) E:\>attrib -s -h 捷徑病毒中毒症狀.png
📬 網路		

1

# **THANK YOU**

## ~ 簡報結束・謝謝~ Thank you for listening