# TRS File Monitor

使用手册





# Team Rise System Co., Ltd.

台北市杭州南路1段8-1號4樓 TEL:02-23221622 FAX:02-23223986 統一編號:96943675

DATE : 2022/09/12

# 目錄

1.	啟重	力 TRS File	e Monitor	4
	1.1	安裝]	TRS File Monitor	4
	1.2	自動力	11入白名單	4
	1.3	警示詞	汛息	5
	1.4	彈出社	見窗	5
	1.5	TRS F	File Monitor 運作畫面	5
2.	TRS	S File Mon	itor 按鈕功能	6
	2.1	卸載利	呈式-Uninstall	6
	2.2	停止傾	貞測-Stop	6
	2.3	白名單	單-White List	6
		2.3.1	從工作管理員中加入常用程式	7
		2.3.2	使用者從檔案路徑加入程式	7
		2.3.3	從被偵測為可疑程式之序列加入白名單	7
	2.4	硬體驗	歲證-Verification	8
		2.4.1	查看本機機碼	8
		2.4.2	開啟硬體驗證	8
		2.4.3	亂數驗證碼	9
	2.5	隔離區	显-Isolation	9
		2.5.1	復原程式-Restore	9
		2.5.2	刪除程式-Delete	9
	2.6	回到背	皆景作業-Hide	10
	2.7	關於-/	About	10
		2.7.1	版本資訊	10
		2.7.2	聯繫 TRS File Monitor 開發團隊	11
		2.7.3	偵測報告	11
		2.7.4	傳送報告給 TRS File Monitor 開發團隊	12
3.	常見問	5題		13

3.1	為什麼要安裝 TRS File Monitor ?13
3.2	TRS File Monitor 免費試用版與付費版之差異。13
3.3	遇到安裝新程式時,被 TRS File Monitor 阻擋,而導致無法順利安裝。13
3.4	TRS File Monitor 經測試,能夠阻擋以下勒索軟體:13
3.5	安裝 TRS File Monitor 的電腦規格需求。13
3.6	強烈建議開啟 UAC (使用者帳戶控制)。14
3.7	為什麼已開啟硬體驗證,仍會被要求輸入機碼?15
3.8	Sever 已安裝 TRS File Monitor,本機未安裝,輸入亂數機碼時,為什麼會直接登出跳回15
3.9	Windows 工作列看不到 TRS File Monitor Icon?16
3.10	按TRS File Monitor的 Stop 可停止監測,是否也會停止防止勒索軟體功能?16
3.11	按結束時或被強迫結束時,是否也會停止防止勒索軟體功能?
3.12	系統登出時,是否也會停止防止勒索軟體功能?16
3.13	如何得知有偵測到可疑勒索軟體行為?16
3.14	驗證(Verification)功能,是針對什麼做驗證?16
3.15	如何用複製(Ctrl+C)與剪貼(Ctrl+V)等功能, 輸入 Server 端驗證碼?
3.16	為何遠端桌面連線(Remote Desktop Connection)的剪貼功能無效?
3.17	開啟合法程式時被誤判為勒索軟體,出現警告訊息,程式無法正常使用?
3.18	突然出現是否將程式加入白名單的訊息,是否該加入?
3.19	執行 Msconfig.exe 修改開機資料無效?
3.20	使用 TRS File Monitor 是否有個資外洩的風險?
3.21	如何建構一個防止勒索軟體的環境

### 1. 啟動 TRS File Monitor

1.2

1.1 安裝 TRS File Monitor

雙擊兩下程式便將會出現使用者帳戶控制之視窗,點選是,即可順利安裝。 安裝成功後,點選確定,TRS File Monitor正式啟動。

$\rightarrow$ $\sim$ $\uparrow$	> TRS File Monitor				
★ 快速存取	名稱	<u>^</u>	修改日期	類型	大小
■ 桌面 🔹	ChkTRSFileMonito	or	2022/2/15 下午 01:28	Windows 批次檔案	1 KB
<u>↓</u> 下載 *	FileMonitor	Information	2022/5/44 TH 02.47	☆田 472 →	X
📑 文件 🔹 🖈	TRS_TEMP.1	TRS File M Monitor\F	Ionitor installed successfully:( ileMonitor.exe	C:\Users\TRS\Desktop\TRS	File B
System32	TRS_TEMP.A			確	定 B
1 音楽	TRS_TEMP.TMP		2021/3/5 正十 08:32	IIVIP 個柔	T KB
■ 需求訪談	🚡 TRSFileService		2021/2/5 下午 03:15	應用程式	914 KB
📒 請勿砍-行程規!	🖉 TRSMsg		2020/10/8 下午 03:17	應用程式	911 KB
<ul> <li>OneDrive</li> </ul>	🖲 TRSWebSite		2021/1/19 上午 11:08	Windows 批次檔案	2 KB
■ <sub>本機</sub> 動加入白名單					
■ 本標 動加入白名單 美成功後,第一	次使用會出現是	上否將目前開展	故中的程式加入自	∃名單,依據⊥	作官理
■ <sup>本機</sup> 動加入白名單 長成功後,第一 TRS File Monitor ① <sup>新増</sup> ~ &	-次使用會出現是 □	E否將目前開題 这───── № #	改中的程式加入自 ☞~ ■ <sup>檢視</sup> ~	∃名單,依據⊥	_作官埋_
■ 本標 動加入白名單 設成功後,第一 TRS File Monitor ① 新増 ~ & - → ~ ↑	·次使用會出現是	と否將目前開題 20	故中的程式加入自 <sub>序~</sub> ≡ <sub>檢視~</sub>	∃名單,依據⊥	_作官理,

三 桌面 \* S File Warning  $\times$ ↓ 下載 4 🌠 Filel Insert you trust program from Task Manager to TRS White List? C:\Windows\System32\smss.exe 🔤 文件 \* Rea 🚬 圖片 \* Yes to <u>A</u>ll <u>Y</u>es <u>A</u>bort <u>N</u>o 🗋 TRS 🚞 System32 0 KB TRS\_TEMP.A 2020/9/13 下午 02:21 A檔案 🚺 音樂 TRS\_TEMP.K 2020/9/13 下午 02:21 K 檔室 0 KB 늘 需求訪談 TRS\_TEMP.TMP 2021/3/5 上午 08:32 TMP 檔案 1 KB 늘 請勿砍-行程規! TRSFileService 2021/2/5 下午 03:15 應用程式 914 KB OneDrive 🖉 TRSMsg 2020/10/8 下午 03:17 應用程式 911 KB 📧 TRSWebSite 2021/1/19 上午 11:08 Windows 批次檔案 2 KB > 💻 本機

按鈕-Yes:依照訊息視窗中的檔案,逐筆加入白名單。 按鈕-No:依照訊息視窗中的檔案,逐筆不加入白名單。 按鈕-Abort:全部略過。 按鈕-Yes to All:全部加入(建議選取)。

4

### 1.3 警示訊息

若於1.2項目中,未選擇[Yes to All],則有可能出現下列訊息。

Warning

#### $\times$



確定	取消

#### 1.4 彈出視窗

若於 1.2 項目中,未選擇[Yes to All],亦有可能出現下列訊息。 TRS File Monitor 若偵測到可疑行為將於螢幕右下方出現視窗,並將該程式移至隔離區。



1.5 TRS File Monitor 運作畫面

TRS File Monitor 於背景作業執行,並不影響使用者操作,可於工具列中點開圖示,則可看見即時偵測畫面,並使用其他按鈕功能。



		TRS Fi	le Monitor - Anti Ran	somware		_ <b>_</b> ×
		ر 🖉	<b>FRS File Moni</b>	tor		
Tuninstall	Stop	White List	<b>Verification</b>	<b>蕾 Isolation</b>	🗟 Hide	? About
	The s	ystem window is trigg	jered, User:= ,Domai	n:=, ExePath:=, Proce	essID:=0	
File Monitor List           2022/9/12 上午 10:13           2022/9/12 上午 10:13           2022/9/12 上午 10:13           2022/09/12 上午 10:13           2022/9/12 上午 10:13	:03>CreateFolde :04>Deleteltem:C 3:04>CreateFold 3:04>CreateFold :07>Modifiltem:C :07>Modifiltem:C :07>Modifiltem:C :07>Modifiltem:C :07>Modifiltem:C :07>Modifiltem:C :07>Modifiltem:C :07>Modifiltem:C :08>Modifiltem:C :08>Modifiltem:C :08>Modifiltem:C :08>Modifiltem:C :08>Modifiltem:C :08>Modifiltem:C :08>Modifiltem:C	r:C:\Users\luce\AppD 2:\Users\luce\AppData er:C:\Users\han\AppData er:C:\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData :\Users\han\AppData	Data Local Temp 10 get a Local Temp 10 get Data Local Microsoft Data Local Microsoft Local Mic	etpaths.cmd baths.cmd Edge\User Data\Defa Edge\User Data\Defa e\User Data\Default\\ e\User Data\Default\\ e\User Data\Default\\ e\User Data\Default\\ e\User Data\Default\\ e\User Data\Default\\\ e\User Data\Default\\\- e\User Data\Default\\-	ult\Code Cache\j letwork Action Pr letwork Action Pr listory-journal listory-journal listory-journal listory-journal	is\index-dir\temp-index is\index-dir\the-real-ind edictor-journal edictor-journal edictor-journal edictor-journal edictor-journal edictor-journal edictor-journal edictor-journal
<		Ш				>

- 2. TRS File Monitor 按鈕功能
  - 2.1 卸載程式-Uninstall

<b></b>	式。							
	TRS Fi	e Monitor - Anti Rans	omware	_ <b>_</b> ×				
	TRS File Monitor							
📄 Uninstall 💿 Stop	White List	<b>&amp; Verification</b>	🖶 Isolation	Hide ? About				
2.2 停止偵測-Stop 點選按鈕後,即停止偵测	則。							
	TRS Fi	e Monitor - Anti Rans	omware	_ <b>_</b> X				
TRS File Monitor								
	-							
Tuninstall 🛞 Stop	White List	<b>%</b> Verification	1 Isolation	)Hide ? About				
<b>Thinstall ● Stop</b> 2.3 白名單-White List	White List	<b>«</b> Verification	Television Television	Hide ? About				
● Stop 2.3 白名單-White List	White List	<b>Verification</b> e Monitor - Anti Ranso	Teleform Teleform	Hide ? About				

🔦 Verification

🖥 Isolation

🛞 Hide

? About

🚽 Uninstall

Stop

🕮 White List

以下有三個方式(紅框處)可將信任程式加入白名單,以避免 TRS File Monitor 誤判,下方藍框則是目前於白名單列表中的程式。

	TRS White List	
	TRS White List	
<b>才 Insert ↓ Delete</b>	Find Find	
Program		h 🔁 🗎
Detect program is installed		
TRS White List] D.\TRS File Monitor\filemonitor.exe c:\Windows\System32\smss.exe= c:\Windows\System32\csrss.exe= c:\Windows\System32\winlogon.ex c:\Windows\System32\winlogon.ex c:\Windows\System32\services.exe c:\Windows\System32\services.exe c:\Windows\System32\services.exe c:\Windows\System32\dwm.exe= c:\Windows\System32\dwm.exe= c:\Windows\System32\tintsvr.exe= c:\Windows\System32\tintsvr.exe= c:\Windows\System32\tintsvr.exe= c:\Windows\System32\tintsvr.exe= c:\Windows\System32\tintsvr.exe=	e=ok ok ok e=ok e=ok ok e=ok k vork64\v4.0.30319\SMSvcHost.exe=ok QL Server\90\Shared\sqlbrowser.exe=ok ok	
<	III	>

2.3.1 從工作管理員中加入常用程式

TRS File Monitor 會從工作管理員偵測常用的程式,直接加入白名單。



2.3.2 使用者從檔案路徑加入程式

使用者可藉由檔案路徑選擇信任之程式加入白名單。



2.3.3 從被偵測為可疑程式之序列加入白名單

TRS File Monitor 會將可疑程式紀錄至 TRS\_Readme.txt 中,使用者點選此按鈕,可加入 被偵測為可疑程式之信任的程式,此按鈕會逐筆顯示是否要加入白名單之訊息。 Warning ×



按鈕-Yes:依照訊息視窗中的檔案,逐筆加入白名單。 按鈕-No:依照訊息視窗中的檔案,逐筆不加入白名單。 按鈕-Abort:全部略過。 按鈕-Yes to All:全部加入(不建議選取)。

#### 2.4 硬體驗證-Verification

TRS File Monitor 提供多人環境 RDP 登錄時驗證使用,可使用硬體驗證功能加層防護。



## 2.4.2 開啟硬體驗證

於遠端主機之 TRS File Monitor 開啟硬體驗證功能(紅色框),只要欲連線之使用者的主機已新增至名單中,進入遠端主機無須登打驗證碼,即可連線。



#### 2.4.3 亂數驗證碼

若使用者未安裝 TRS File Monitor,欲連線至遠端主機,除了需輸入原本 RDP 連線之使用者帳密外,也須按照客製化之亂數輸入機碼,才可成功進入遠端主機。



# 2.5 隔離區-Isolation

當應用程式出現類勒索軟體行為時,將有可能被移至隔離區,以保護使用者作業環境。

		TRS Fil	le Monitor - Anti Ran	somware		_ <b>D</b> X
		т 🕎	RS File Moni	tor		
💂 Uninstall	Stop	💭 White List	<b>%</b> Verification	<b>壶 Isolation</b>	🗟 Hide	? About

# 2.5.1 復原程式-Restore

若信任的程式被加入至隔離區導致無法順利執行時,可於隔離區復原,程式將自動加入白名單,並將程式回復到原來安裝的路徑。

# 2.5.2 删除程式-Delete

若隔離區出現可疑程式,可直接透過 TRS File Monitor 删除該程式。

	TRS Isolation	
Ļ	TRS Isolation	
Telete Restore CRefresh		
Sel	lect program to delete or restore	
CreateTime:2022/05/06,14:30:12,Program:SF CreateTime:2022/05/18,15:23:41,Program:TF CreateTime:2022/06/02,17:10:32,Program:so CreateTime:2022/06/13,17:14:22,Program:vs CreateTime:2022/06/20,10:26:53,Program:PE	KCOMTester.vshost.exe,Path:D:\TRS File Monitor\TRSBackup\Isola RSBond.Bloomberg.Mantis.WinForm.vshost.exe,Path:D:\TRS File M oftware_reportskexe,Path:D:\TRS File Monitor\TRSBackup\Iso stest.dig_vvexengine x3xe,Path:D:\TRS File Monitor\TRSBackup\Isolation DFRENT1	ation\D\\^ Ionitor\T Iation\C\ \Isolatio ROGRA
٢ ١١		>

# 2.6 回到背景作業-Hide

使用者若要隱藏 TRS File Monitor 於桌面,可點選 Hide,讓程式回到背景作業,此動作並不影響偵測進行。

		TRS Fi	le Monitor - Anti Rans	somware		_ 🗆 X
		r 🗳	<b>RS File Moni</b>	tor		
ᡖ Uninstall	Stop	White List	<b>Nerification</b>	Tsolation	🗟 Hide	? About

#### 2.7 關於-About

TRS File Monitor 版本資訊位於此頁籤,可提供使用者確認當前是否為最新版本。

		TRS Fi	le Monitor - Anti Rans	somware		_ <b>D</b> X
		1 🛒	<b>TRS File Monit</b>	tor		
📄 Uninstall	Stop	C White List	<b>%</b> Verification	<b>∄</b> Isolation	🖓 Hide	? About

2.7.1 版本資訊

若使用者本機之版本非為最新版本,則會跳出提示視窗,且紅框處為試用剩餘天數。 Infomation ×





# 2.7.2 聯繫 TRS File Monitor 開發團隊

可點選網址進入官方網站,藉以更瞭解本產品及聯繫我們。

About	$\times$
TRS File Monitor	
Version: 2.4.0.0 (Trial) 90 days	
Copyright: Team Rise System Co., Ltd.	
Mail TRS_Readme.txt to us	
https://www.teamrise.com.tw/trsfilemonitor/	<u>/</u>
Purpose(Anti Ransomware):	
1. Prevent ransomware encrypt file names or contents.	
2. Prevent ransomware modify BCD (Boot Configuratio:	
3. Prevent beforehand instead of anti-decryption afterwa	
4. Protect your computer when the operating system boc	
5. Suitable for all windows os.	
6. Free trial software for 90 days.	
You can pay for the "Official Use Authorization Letter'	

# 2.7.3 偵測報告

TRS File Monitor 將會記錄時間與發生疑似勒索行為之檔案列表,可於此按鈕產生清單, 提供後續追蹤。

About	<
TRS File Monitor	
Version: 2.4.0.0 (Trial) 90 days	
Copyright: Team Rise System Co., Ltd.	
Mail TRS_Readme.txt to us	
https://www.teamrise.com.tw/trsfilemonitor/	
<ul> <li>Purpose(Anti Ransomware):</li> <li>1. Prevent ransomware encrypt file names or contents.</li> <li>2. Prevent ransomware modify BCD (Boot Configuratio)</li> <li>3. Prevent beforehand instead of anti-decryption afterwa</li> <li>4. Protect your computer when the operating system boot</li> <li>5. Suitable for all windows os.</li> <li>6. Free trial software for 90 days. You can pay for the "Official Use Authorization Letter"</li> </ul>	

			~
Its_Keadme - iE单本	_		
檔案(F) 編輯(E) 格式(O) 檢視(V) 説明			
1022/6/28 下午 03:53:26>DeleteItem:C:\Users\TRS\AppData\Local\Microsoft\OneDrive\logs\Personal\SyncEngine-2022-06-28.0608.8744.2.0	d 1		
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Users\TRS\AppData\Local\Microsoft\OneDrive\OneDrive.exe, ProcessID:=12524, 0-ExePa	th 1=		
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Program Files (x86)\Google\Chrome\Application\chrome.exe, ProcessID:=7180, 0-ExePa	th1=C:\	Progra	am F
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Program Files (x86)\Google\Chrome\Application\chrome.exe, ProcessID:=16292, 0-ExeP	ath1=C:	\Prog1	ran 🛛
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Users\TRS\Desktop\TRS File Monitor\excel.exe, ProcessID:=8880, 0-ExePath1=C:\Users	\TRS\De	esktop'	ATRS
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Users\TRS\Desktop\ver2.3.0.0\excel.exe, ProcessID:=1384, 0-ExePath1=			
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Program Files (x86)\Google\Chrome\Application\chrome.exe, ProcessID:=13184, 0-ExeP	athl=C:	Prog	ram
ser:=TRS ,Domain:=LAPTOP-SMRAAKAD, ExePath:=C:\Program Files (x86)\Google\Chrome\Application\chrome.exe, ProcessID:=11464, 0-ExeP	athl=C:	Prog	ram
ser:=IRS ,Domain:=LAPIOP-SMRAAAAD, ExePath:=U:\Program Files (x86)\Google\Chrome\Application\chrome.exe, ProcessID:=13564, U-ExeP	athl=C:	Prog	ram
ser:=IRS ,Domain:=LAPIOP-SMRAAAAD, ExePath:=C:\Program Files (x86)\Google\Chrome\Application\chrome.exe, ProcessID:=11732, U-ExeP	athl=C:	Prog	ram
ser:=IKS ,Domain:=LAPIOP-SMKAAKAD, ExePath:=U:VProgram Files (x8b)VoogleVChromeVapplication/chrome.exe, ProcessID:=4092, U-ExePa	εμ I≡C:Λ	Progra	am F I
ser:=IKS ,Domain:=LAPIOP-SMKAAKAD, ExePath:=U:\Program Files\mcafee\WebAdvisor\browserhost.exe, ProcessID:=2776, U-ExePathI=U:\Wi	udo#s/2	ystem:	32\c
ser:=IRS ,Domain:=LAPIOP-SMRAARAD, ExePath:=L:\Program Files (x86)\Voogle\ChromeApplication\Chrome.exe, ProcessID:=9544, U-ExePa	th I=C: \	Progra	am F
ser:=IKS , Domain:=LAPIOF-SMKAAAAD, Exerath:=C:Program Files (x80)\Google\Chrome\Application\Chrome.exe, ProcessiD:=I5350, U-Exer	atni=C:	Progr	ram
ser:=IKS , Domain:=LAPIOF-SMKAAAAD, Exerath:=C:Program Files (x80)\Google\Chrome\Application\Chrome.exe, ProcessiD:=4004, U-Exera	CU I=C:\	Progra	am F
ser:=IKS , Domain:=LAPIOF-SMKAAAAD, Exerath:=L:Program Files (x80)\Google\Chrome\Application\Chrome.exe, ProcessiD:=4005, U-Exera	CD I=C:\	Progra	am F
set:=IKS, JOmain:=LAFIUP-SMKARAAD, Exerath:=L:\Frogram Files (x80)\Usedue(LhromeApplication\Chrome.exe, Processil)=5/84, U-Exerat	ίn i=∪:∖	Progra	im r
set:=iks, Jonain:=Lariur-Snkaanab, Exeratn:=::vrogram riles (xob)\voogle\LhtomeApplication\chtome.exe, Processil:=508, 0-ExePat		rograi	4 F 1
set:=IKS, JOMAIN:=LAFIOF-SMRARAAD, EXErath:=L:\Frogram Files (xoo)\Google\LhomeApplication\Chrome.exe, FrocessiD:=Sido, O-Exerat	11⊒∪:\P +b1⊒C+\	Tograi	a 1° 1
ser:=rs, jourain:=partor-smannab, exergin:=p:vrogram riles (xo0)/Google/Chrome/Application/Chrome.exe, ProcessiD:=2544, U-Exerg	uu=C:\	W LILGON	/sie

# 2.7.4 傳送報告給 TRS File Monitor 開發團隊

若對偵測報告有疑惑之時,可藉由此方式傳送報告供開發團隊,進一步與您聯繫。 ※此內容無個資外洩之風險

About X		
TRS File Monitor		
Version: 2.4.0.0 (Trial) 90 days		
Copyright: Team Rise System Co., Ltd.		
<u>Mail TRS_Readme.txt to us</u>		
https://www.teamrise.com.tw/trsfilemonitor/	Information	×
Purpose(Anti Ransomware):         1. Prevent ransomware encrypt file names or contents.         2. Prevent ransomware modify BCD (Boot Configuration)         3. Prevent beforehand instead of anti-decryption afterwa         4. Protect your computer when the operating system boc	Mail is sended.	^
<ol> <li>Suitable for all windows os.</li> <li>Free trial software for 90 days. You can pay for the "Official Use Authorization Letter'</li> </ol>	確定	T

- 3. 常見問題
  - 3.1 <u>為什麼要安裝 TRS File Monitor ?</u>
    - 以不同於其他防毒或防勒索軟體的觀念與方法,能阻擋全球知名的防毒或防勒索軟體無法阻擋的 Ransomware。
    - 偵測到可疑 Ransomware 行為時,及時甚至事先阻擋檔案被變更。
    - 從一個平常的建立或更名或刪除檔案行為,即能判斷是否為可疑的 Ransomware。
    - 預防 Ransomware 修改 BCD(啟動組態資料庫)。
    - 針對 RDP(遠端桌面連線)多一層防護。
  - 3.2 TRS File Monitor 免費試用版與付費版之差異。

功能	免費試用版	付費版
偵測與預防勒索行為	$\checkmark$	$\checkmark$
專人服務	×	$\checkmark$
客製化服務	×	✓ (詳如 <u>3.21</u> )
授權書	×	$\checkmark$
使用期限	<b>90</b> 天	年費制
不論免費試用或付費版本	,資訊安全沒有絕對安全,都需要	吏用者回饋,讓功能與時俱進。

- 3.3 遇到安裝新程式時,被 TRS File Monitor 阻擋,而導致無法順利安裝。
  - 於 White List 頁籤中勾選 [Detect Program is installed],不須結束程式,但為了安全性安裝 程式後,記得勾選回 [Detect Program is installed]

	TRS White List	l	_ <b>D</b> X
	TRS White List		
≠i Insert ±i Delete ⊯	Find Find		
Program			🐴 🔁 👸
Detect program is installed			
TRS White List] D.\TRS File Monitor\filemonitor.exe= c:\Windows\System32\smss.exe=ok c:\Windows\System32\srss.exe=ok c:\Windows\System32\winlogon.exe= c:\Windows\System32\services.exe= c:\Windows\System32\services.exe= c:\Windows\System32\services.exe= c:\Windows\System32\dwm.exe=ok c:\Windows\System32\dwm.exe=ok c:\Windows\System32\dwm.exe=ok c:\Windows\System32\dwm.exe=ok	ok sok ok ok rk64\v4.0.30319\SMSvcHost.exe=ok . Server\90\Shared\sqlbrowser.exe=ok		
			~
	III		>

● 可以直接點選 Stop 按鈕(如 2.2),停止偵測,安裝成功後,再點選 Start 恢復偵測。

3.4 TRS File Monitor 經測試,能夠阻擋以下勒索軟體:

Reveton、CryptoLocker、TorrentLocker、CryptoWall、KeRanger、RSA4096、Mischa、WannaCr ypt、Petya、Bad Rabbit 等,有助於使用者於安全環境下正常執行。

#### 3.5 安裝 TRS File Monitor 的電腦規格需求。

- Microsoft Windows Server 2008 Standard 以上(包含 x86、x64)
- Microsoft Windows 7 家用進階版以上(包含 x86、x64)
- 強烈建議開啟 UAC(使用者帳戶控制),詳如 3.6 章節。

3.6 <u>強烈建議開啟 UAC (使用者帳戶控制)。</u>

Step1:於電腦搜尋工具輸入-控制台

搜尋	
每個地方 🗸	
控制台	<mark>م</mark>
空間	

Step2:點擊[使用者帳戶]

9	
(③) ⊘) ▽ ↑ 📴 ▶ 控制台	✓ C 授尋控制台 ○
調整電腦設定	檢視方式: 類別 ▼
系統及安全性 檢閱您的電腦狀態 發檢視事件記錄檔	使用者帳戶
網路和網際網路 檢視網路狀態及工作	外觀 變更桌面窝景 調整螢幕解析度
使 體 檢視裝置和印表機 新增裝置	時鐘、語言和區域 新增語言 變更動入法
程式集 解除安礙程式 愛 關欽或關閉 Windows 功能	設定時間和口胡 變更日期、時間或數字格式 輕鬆存取 讓Windows 速邁設定 最佳化提營顯示

Step3:再次[選取使用者帳戶]

<u>\$8</u>	使用者帳戶	_ <b>□</b> ×
ⓒ ② ▼ ↑ 🍇 ▶ 控制台	,使用者帳戶	<ul><li> ・ C 授尋控制台 ・ ク </li></ul>
控制台首頁	使用者帳戶 ◎ 變更帳戶類型   ◎ 移除使用者帳戶	
網路和網際網路 硬體	認證管理員 管理網站認證   管理 Windows 認證	
程式集 ● 使用者帳戶	↓ 郵件	
外觀 時鐘、語言和區域		
輕鬆存取		

Step4: 開啟 UAC (使用帳戶控制), 選取[變更使用者帳戶控制設定]



Step 5: 將左邊拉回初始值如下方紅框位置,再選取[確定]

<b>()</b>	使用者帳戶控制設定	_ 🗆 X
選擇電腦變更的 「使用者帳戶控制」 顯示使用者帳戶控制	]通知時機 可協助防止可能有害的程式變更您的電腦。 設定的詳細資訊	
—律通知 — — — —————	只在應用程式嘗試變更我的電腦時才通知我 (預設值) ● 當我變更 Windows 設定時 <sup>,</sup> 不要通知我。	
	若使用熟悉的應用程式並瀏覽熟悉的網站則建議使     用。	
不要通知		
	🚱 確定	取消

Step 6: 需重新啟動電腦,設定才會生效。

- 3.7 <u>為什麼已開啟硬體驗證,仍會被要求輸入機碼?</u>
  - 可先檢查本機機碼,是否已加入至 Sever 的 TRS File Monitor 驗證清單列表中。
  - 確認 TRS File Monitor 是否已安裝。
  - 查看 TRS File Monitor 是否停止偵測,詳如 2.2 章節。
  - Windows 遠端桌面連線(Remote Desktop Connection)的剪貼簿功能必須勾選,才能做 Client 端硬體驗證,詳如 <u>3.14</u>章節。
- 3.8 Sever 已安裝 TRS File Monitor,本機未安裝,輸入亂數機碼時,為什麼會直接登出跳

回本機?

● TRS File Monitor 為防止駭客攻擊,則將與機碼無關之按鍵鎖定,一旦使用者觸擊,則開

啟保護模式,直接從 Sever 登出。

- 使用者僅能使用: "Ctrl"、英文、數字、"-"等按鍵,除此以外則視為駭客攻擊。
- 按了 ALT 等鍵,嘗試離開驗證畫面。
- 為了防止駭客使用各種方式猜對亂數機碼,系統設定30秒內完成輸入,30秒後未輸入 完成,即登出。
- 3.9 Windows 工作列看不到 TRS File Monitor Icon?
  - 使用者權限不足,安全性考量,系統管理者才能看到與使用。
  - 因開機不須登入即已啟動保護,所以有時在控制台(Console Mode)模式下,系統管理者 登出再取消登出,即能看到。
- 3.10 按 TRS File Monitor 的 Stop 可停止監測,是否也會停止防止勒索軟體功能?

在單人模式是:但在多人環境(Multi Session)下,仍舊保有防止勒索軟體功能。

3.11 按结束時或被強迫結束時,是否也會停止防止勒索軟體功能?

按結束時或被強迫結束時,會自動再被啟動,除非人工解除安裝(Uninstall)。

3.12 <u>系統登出時,是否也會停止防止勒索軟體功能</u>?

系統登出時,仍舊保有防止勒索軟體功能;在控制台(Console Mode)模式下,系統登出時會出現警示訊息,亦不會影響防止勒索軟體功能。

- 3.13 如何得知有偵測到可疑勒索軟體行為?
  - 登入狀態下會出現下列警告訊息畫面,詳如<u>1.4</u>章節。
  - 進入隔離區可看到依日期排序被隔離的程式,如程式重複被隔離僅會顯示第一次的日期, 詳如 2.5章節。
  - 點擊 About 的 mail 圖示可看到可疑勒索軟體行為與隔離記錄,詳如 2.7.3 章節。
- 3.14 <u>驗證(Verification)功能,是針對什麼做驗證?</u>
  - 專門針對 Windows 遠端桌面連線(Remote Desktop Connection)登入做 Client 端或 Server 端硬體驗證,防止使用者密碼被駭時,多一層更嚴密保護,讓行動辦公或遠端登入更安全,詳如 2.4 章節說明。
  - Client 端若未安裝 TRS File Monitor , 例如用手機 RDC APP 登入, 會自動做 Server 端硬體 驗證。
  - Client 端若有安裝 TRS File Monitor 時會自動驗證,不需輸入驗證碼,但驗證失敗時,亦 會啟動 Server 端硬體驗證,可等 30 秒自動登出後再重新登入即可。
  - Windows 遠端桌面連線(Remote Desktop Connection)的剪貼簿功能必須勾選,才能做 Client 端硬體驗證。如圖示

100 遠端桌面連線	_		×
<b>运</b> 端桌面			
──── 連線			
一般 顯示 本機資源 效能體驗 進階			
這端音訊			
設定遠端音訊。			
設定( <u>S</u> )			
鍵盤			
套用 Windows 按鍵組合( <u>K</u> ):			
只有在使用全螢幕時	~		
範例: ALT+TAB			
本機裝置和資源			
選擇遠端工作階段中要使用的裝置與資源。 200			
✓ 印表機①			
其他( <u>M</u> )			
▲ 陽藏選項(Q)	D	說明(	Ð

● Client 端或 Server 端硬體 TRS Verification Key 可隨時更改 Hard Disk C:磁碟的 Label 來變動 TRS Verification Key 的某一部份,以增加安全性。如圖示

Step1:更改前,使用系統管理員身分開啟 cmd 查詢當前 label 值,輸入: label



Step2:並以 2.4.1 章節方式開啟本機機碼

TRS File Monitor	×
00-0E-C6-B9-AB-13OS14C0	)15B0
ОК	

Step3: 輸入欲更改之磁碟區名稱:TEXT (範例)



Step4:以2.4.1章節方式查詢更正後的機碼

TRS File Monitor	×
00-0E-C6-B9-AB-13TEXT14C015B	0
ОК	

- Server 端啟動驗證功能時,若忘記 TRS Key 導致系統無法登入時,可由本機控制台進入, 取得或設定 TRS Verification Key。詳 2.4.1 章節。
- RDC 斷線時必須設定即時登出,如圖示
   Step1:先開啟「群組物件原則編輯器」,輸入gpedit.msc

	執行	x
	睮入程式、資料夾、文件或網際網路資源的名稱,Window 會自動開啟。	NS
開啟(O):	gpedit.msc	~
	確定 取消 瀏覽(B)	

Step2:找到本機電腦原則/電腦設定/系統管理範本/Windows元件/遠端桌面服務 (終端機服務)/工作階段,選取"設定已斷線工作階段的時間限制"



Step3:設定已斷線工作階段的時間限制,勾選已啟用、設定分鐘數(依使用者狀況自行 選擇)

<b>.</b>	設定已斷線工作階段的時間限制	×
設定已斷線工作階段的時間限制	上一個設定(P) 下一個設定(N)	
○ 尚未設定( <u>C</u> ) 註解: ● 已飲用( <u>E</u> )		^
○ 已停用( <u>D</u> ) 支援的作業系統:	至少需要 Windows Server 2003 作業系統或 Windows XP Professional	$\sim$
選項:	說明:	
終止已中斷連線的工作階段 1 分鐘 v	這個原則設定可以讓您為已中斷連線的遠端桌面服務工作階段設定時間限制。 您可以使用這個原則設定,指定已中斷連線的工作階段在伺服器上保持使用中狀態的時間上限。根據預設,遠端桌面服務允許使用者不須登出及結束工作階段,就可以中斷與遠端桌面服務工作階段的連線。 當工作階段處於中斷連線狀態時,即使使用者目前已不在連線中的狀態	<
	這些已中斷連線的工作階段。 如果您啟用這個原則設定,經過指定的時間後會將已中斷連線的工作階段從伺服器中刪除。若要強制使用預設行為(無限期保留中斷連線的工作 階段),請選取[永不]。如果您有主控台工作階段,則不適用已中斷連線 工作階段的時間限制。	
	如果您停用或未設定這個原則設定,則不會在群組原則層級指定這個原 則設定。根據預設,遠端桌面服務已中斷的工作階段會被無限期保留。	~
	<b>確定</b> 取消 套用(A)	

● Servser 端硬體 TRS Verification Key 驗證碼須搭配動態值輸入,以增加安全性。

#### 3.15 <u>如何用複製(Ctrl+C)與剪貼(Ctrl+V)等功能, 輸入 Server 端驗證碼?</u>

必須在出現 Server 端驗證畫面時,切換至 Client 端,複製(Ctrl+C)字串,再切換至 Server 端驗證畫面,在驗證欄位剪貼(Ctrl+V)字串。

3.16 <u>為何遠端桌面連線(Remote Desktop Connection)的剪貼功能無效?</u>

啟用驗證(Verification)功能時,必須登入驗證後,剪貼功能才能正常使用。

3.17 <u>開啟合法程式時被誤判為勒索軟體,出現警告訊息,程式無法正常使用?</u>

可至隔離區(Isolation)將該程式恢復(Restore)即可正常使用,詳如 2.5 章節。

3.18 突然出現是否將程式加入白名單的訊息,是否該加入?

如果訊息是由人工開啟程式過程中即時出現的,例如使用者開啟記事本時,出現此訊息,可安心加入記事本於白名單,以避免程式在執行過程中被強迫結束,如圖示

×	-		新増 文字文件	
ŝ			編輯	檔案
				1
		Warning		
		Insert you trust program to TRS White List? C\Program Files\WindowsAppsMicrosoft.WindowsNotepad_11.2205.11.0_x64_8we kyb3d8bbwe\Notepad\Notepad.exe		
		福定 取消		
		Warning X Insert you trust program to TRS White List? C.\Program Files\WindowsApps\Microsoft.WindowsNotepad_11.2205.11.0_x64_8we kyb3d8bbwe\Notepad\Notepad.exe		

#### 3.19 <u>執行 Msconfig.exe 修改開機資料無效?</u>

因未對下列訊息做確認,如圖示

۹				系統設定			х
一般	開機 服務	し しゅうしん しゅうしゅう しゅうしゅう しゅうしん しゅう しゅうしん しゅう	具				
Wind	ows Server 2012	R2 (C:\Wind	ows) · 目前的 C	S· 預設 OS			
	進階選項(⊻)	設成	定成預設值( <u>S</u> )	刪除(D)	)		
一開機	選項					等候時間①:	
	安全開機(E)		□無(	GUI 開機( <u>N</u> )		20 秒	
	○ 最基本安全開	機方式( <u>M</u> )	□ 開機	機記錄(B)			
	○ 替代殻層(L)		□基4	⊾視訊(E)			
	<ul> <li>Active Director</li> </ul>	ory 修復(P)	OS	開機資訊( <u>O</u> )		讓所有開機設定永久有效(K	)
	○ 網路(₩)						
				確定	取消	套用( <u>A</u> ) 說明	3



WARNING! from Subsystem (Windows BCD save changes? )
TRS File Monitor Detected that windows BCD was changed! Windows 開機管理程式 
device partition=\Device\HarddiskVolume2 path \EFI\MICROSOFT\BOOT\BOOTMGFW.EFI description Windows Boot Manager locale zh-TW inherit (globalsettings) bootshutdowndisabled Yes default (current)
resumeobject {49aa82b8-57ba-11e6-92df-a146b94bbeef} displayorder {current} toolsdisplayorder {memdiag} timeout 20 Windows 開機載入器
identifier {current} device partition=C: path \Windows\system32\winload.efi description Windows Server 2012 R2 locale zh-TW inherit {bootloadersettings} recoverysequence {49aa82ba-57ba-11e6-92df-a146b94bbeef} recoveryenabled Yes isolatedcontext Yes allowedinmemorysettings 0x15000075 osdewice partition=C: systempont \Windows
resumeobject {V9aa82b8-57ba-11e6-92df-a146b94bbeef} nx OptOut bootmenupolicy Legacy hypervisorlaunchtype Auto 確定 取満

3.20 使用 TRS File Monitor 是否有個資外洩的風險?

不同於其他軟體會將使用者電腦各種資訊傳回,TRS File Monitor 不連線外部任何主機, 徹底杜絕個資外洩的風險(縱然是經由使用者允許, 寄回可疑勒索行為記錄協助判讀時亦

- 然),遵循歐盟防止個資外洩的規範。
- 3.21 如何建構一個防止勒索軟體的環境
  - 良好的備份與還原(即時/批次/異地)
     依可接受的風險,做合理的設備投資。
  - 落實資安政策管理(windows 設定/權限管理/防火牆管理)
    - 1. windows 設定:啟動 UAC(User Account Control)等。
    - 2. 權限管理:儘量不以系統管理者權限登入。
    - 3. 防火牆:定期檢視硬體與軟體防火牆,管制 DNS 與 IP 及 Port 等。
  - 安裝 TRS File Monitor-Anti Ransomware 能對防火牆(port 135/139/445), PSEXEC、PowerShell、BCD(Boot Config Database)、API Hook、遠端桌面連線(Remote Desktop Connection)、DOS Command(Regedit、WMIC...)及 可疑勒索行為等,做有效防護。