新北市政府教育局
資訊安全整合防護委外服務計畫

教育訓練簡報
(防毒服務)

趨勢科技防毒服務

摘要

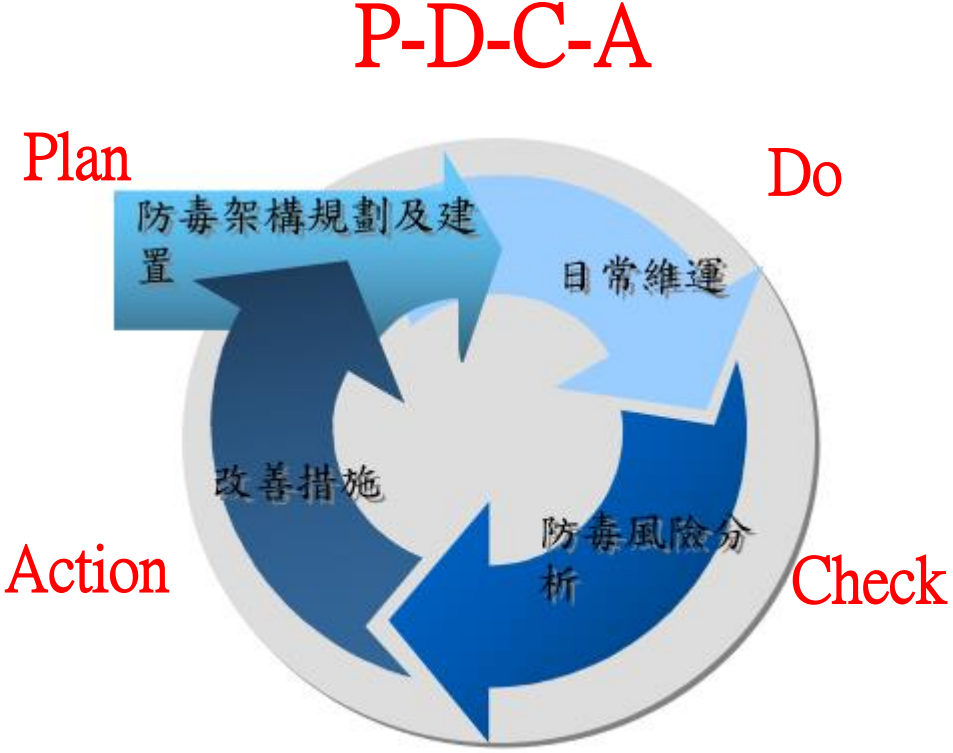
- ESO 服務說明
  - 服務說明
  - 介面總覽
  - 病毒處理流程總覽
  - 病毒處理流程細項介紹
  - 用戶端安裝流程與注意事項
  - SOC 入口網站可查詢到病毒資訊
- 勒索軟體與行動裝置安全
  - 勒索軟體防護與解密工具
  - 行動裝置安全與上網安全
- APEXONE用戶端畫面說明

ESO 服務

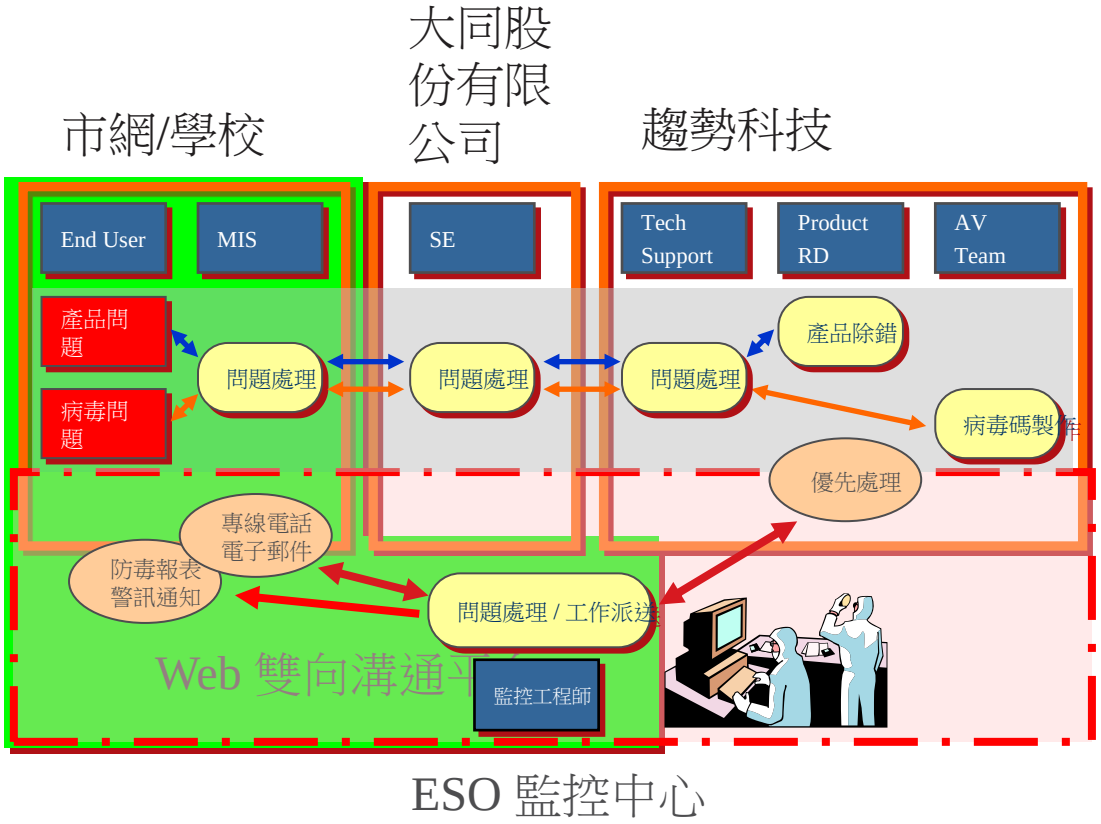
- 服務說明
- 介面總覽
- 病毒處理流程總覽
- 病毒處理流程細項介紹
- 其他說明

服務說明

- 專屬惡意程式清除工具
- 專屬網站及防毒管理系統
- 專屬案件管理系統
- 防毒架構規劃建置
- 專屬技術支援



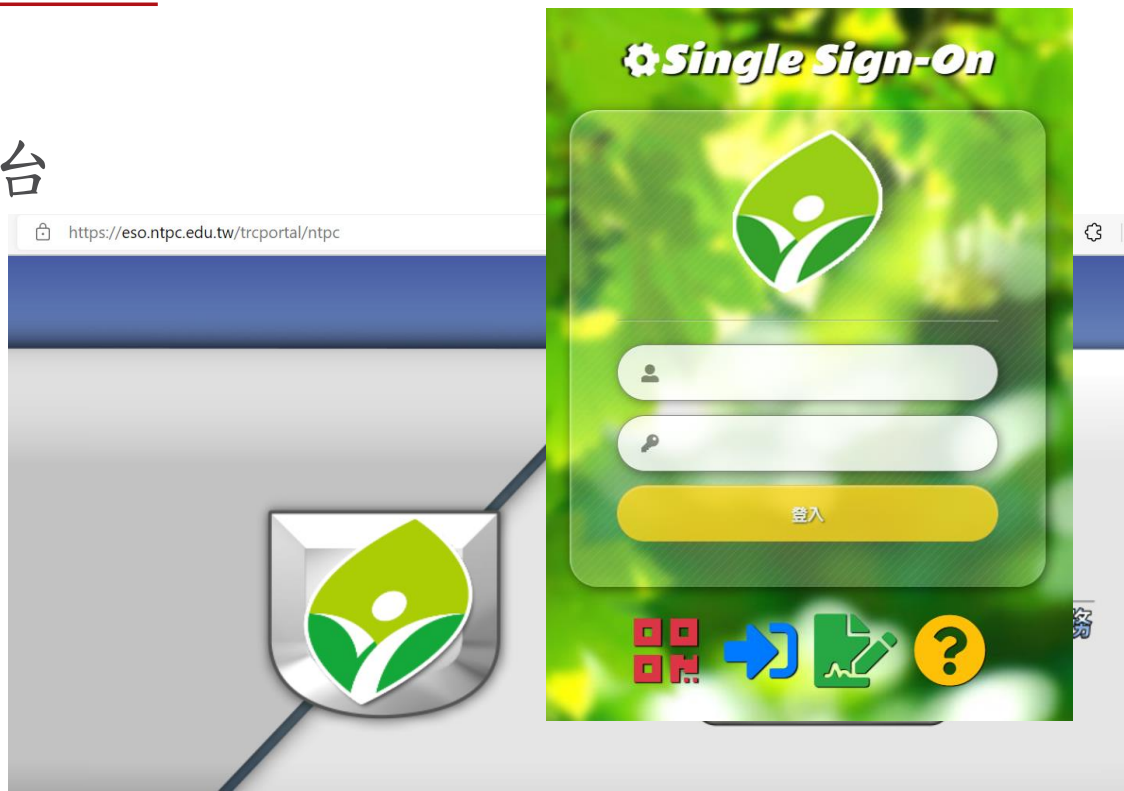
專屬技術支援


大同股份有限公司
市網/學校
趨勢科技
End User
MIS
SE
Tech Support
Product RD
AV Team
產品問題
病毒問題
問題處理
問題處理
問題處理
產品除錯
病毒碼製作
優先處理
專線電話
電子郵件
防毒報表
警訊通知
問題處理 / 工作派送
Web 雙向溝通平
監控工程師
ESO 監控中心

服務說明

https://eso.ntpc.edu.tw（支援SSO）

- 客製化清除工具
- 提供多管道諮詢平台
- 病毒處理程序簡化
- 快速的回應機制
- 提升服務品質



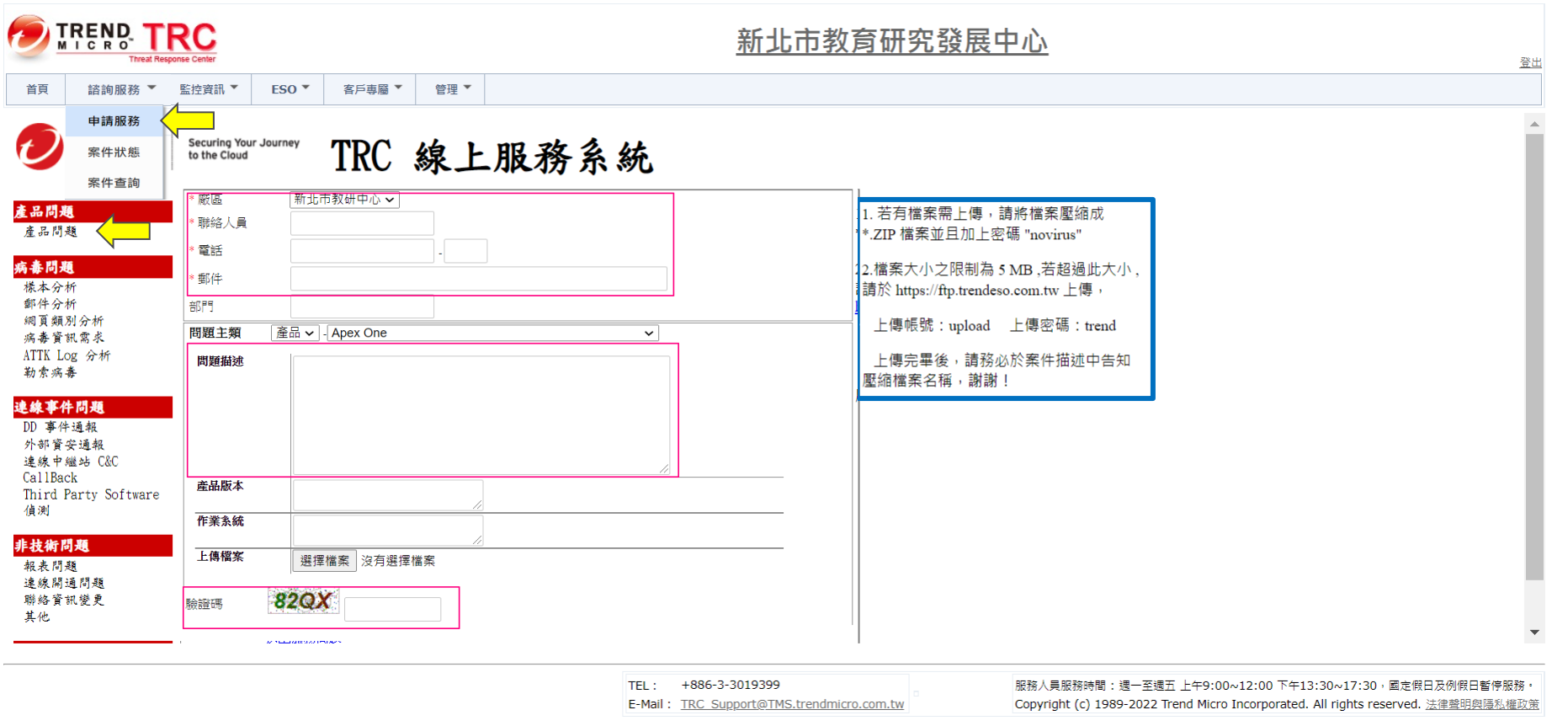
介面總覽

- 首頁

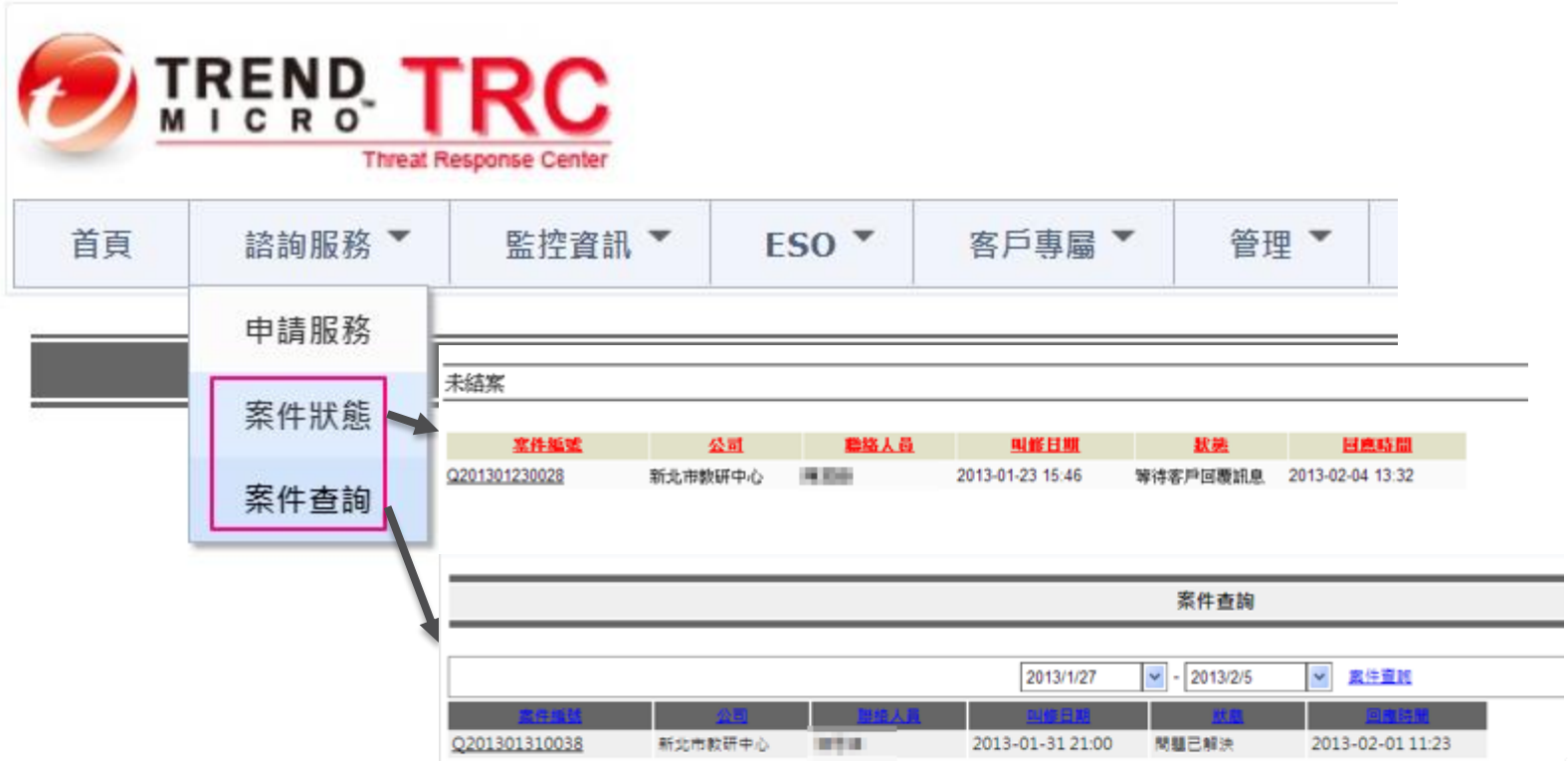
TEL： +886-3-3019399
E-Mail： TRC_Support@TMS.trendmicro.com.tw

服務人員服務時間：週一至週五 上午9:00~12:00 下午13:30~17:30，國定假日及例假日暫停服務。

案件管理系統（各校有專屬登入帳號）

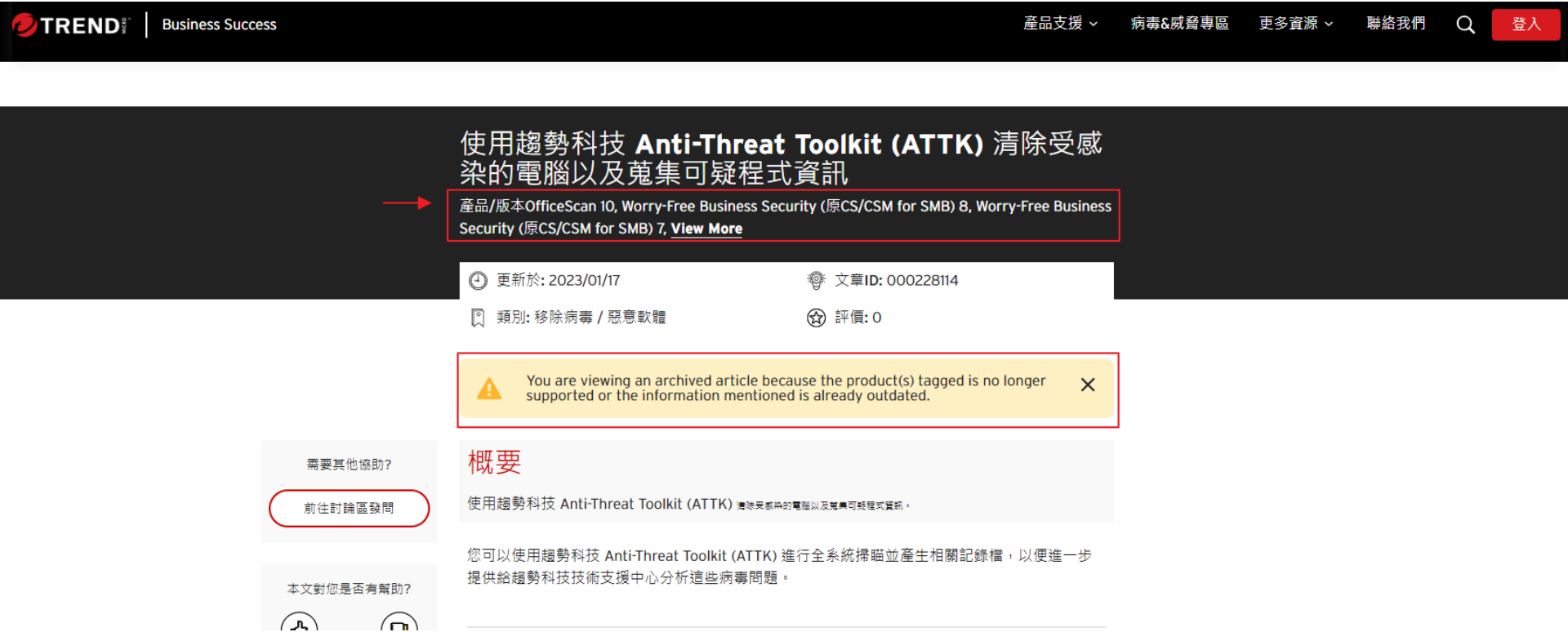


案件管理系統（各校有專屬登入帳號）



防毒相關工具(Anti-Threat ToolKit)

防毒相關工具(ATTK)下載



- 此注意通知在於所列適用產品/版本皆已EOS，非指ATTK工具無法使用，後續會在更新上述資訊，目前ATTK工具仍可正常使用。

防毒相關工具(ATTK)下載

TREND MICRO 企業用戶技術支援

登入 MySupport

技術支援 ▾ | 病毒&威脅專區 | 續約&註冊 | 聯絡我們 | 搜尋

使用趨勢科技 Anti-Threat Toolkit (ATTK) 清除受感染的電腦以及蒐集可疑程式資訊

更新於: 13 Mar 2020 產品/版本: OfficeScan 10.0 , 作業系統: Windows 2003 Enterprise,

概要

使用趨勢科技 Anti-Threat Toolkit (ATTK) 清除受感染的電腦以及蒐集可疑程式資訊。

詳情

您可以使用趨勢科技 Anti-Threat Toolkit (ATTK) 進行全系統掃瞄並產生相關記錄檔，以便進一步提供給趨勢科技技術支援中心分析這些病毒問題。

評價:
20 覺得本文很有幫助。

分類:
移除病毒 / 惡意軟體

解決方案ID:

清除受感染的電腦

1. 請依照受感染電腦的網路環境，下載合適的 Anti-Threat Toolkit (ATTK)
   - 可上網的電腦（32位元）
     可上網的電腦（64位元）
   - 無法上網的電腦（32位元）
     無法上網的電腦（64位元）
2. 閱讀網頁上的授權協議後，點選【I Accept】開始下載工具。
3. 如果出現儲存或執行的訊息視窗，請點選【儲存】。
4. 請將工具儲存到桌面上。
5. 用滑鼠點選兩下儲存到桌面下載的程式 以開始執行。

注意：

(1) 可上網的電腦（32位元）下載的 Anti-Threat Toolkit (ATTK)檔案名稱為：attk_ScanCleanOnline_gui_x86.exe

attk_ScanCleanOnline_gui_x86.exe

- 可上網的電腦（32位元）
- 可上網的電腦（64位元）
- 無法上網的電腦（32位元）
- 無法上網的電腦（64位元）

TREND MICRO

ATTK

- 工具說明

主要功能

- 有效清除近期台灣地區常見的變種病毒、木馬及惡意程式。
- 防止持續變種的惡意程式再次寫入電腦系統中。
- 可收集可疑檔案、系統相關資訊及趨勢科技防毒軟體病毒記錄檔，並可回傳趨勢科技技術服務中心作進一步分析。

ATTK並非是使用防毒軟體的病毒碼，而是針對常見的惡意程式檔案機碼進行刪除及運用新功能TDME追蹤重點檔案的關聯程序及追蹤重點惡意DNS 查詢關聯，並刪除。

重要:ATTK不定時更新並放到下載路徑，需要才下載！

學校端防毒管理步驟

1. 處理學校用戶端需求

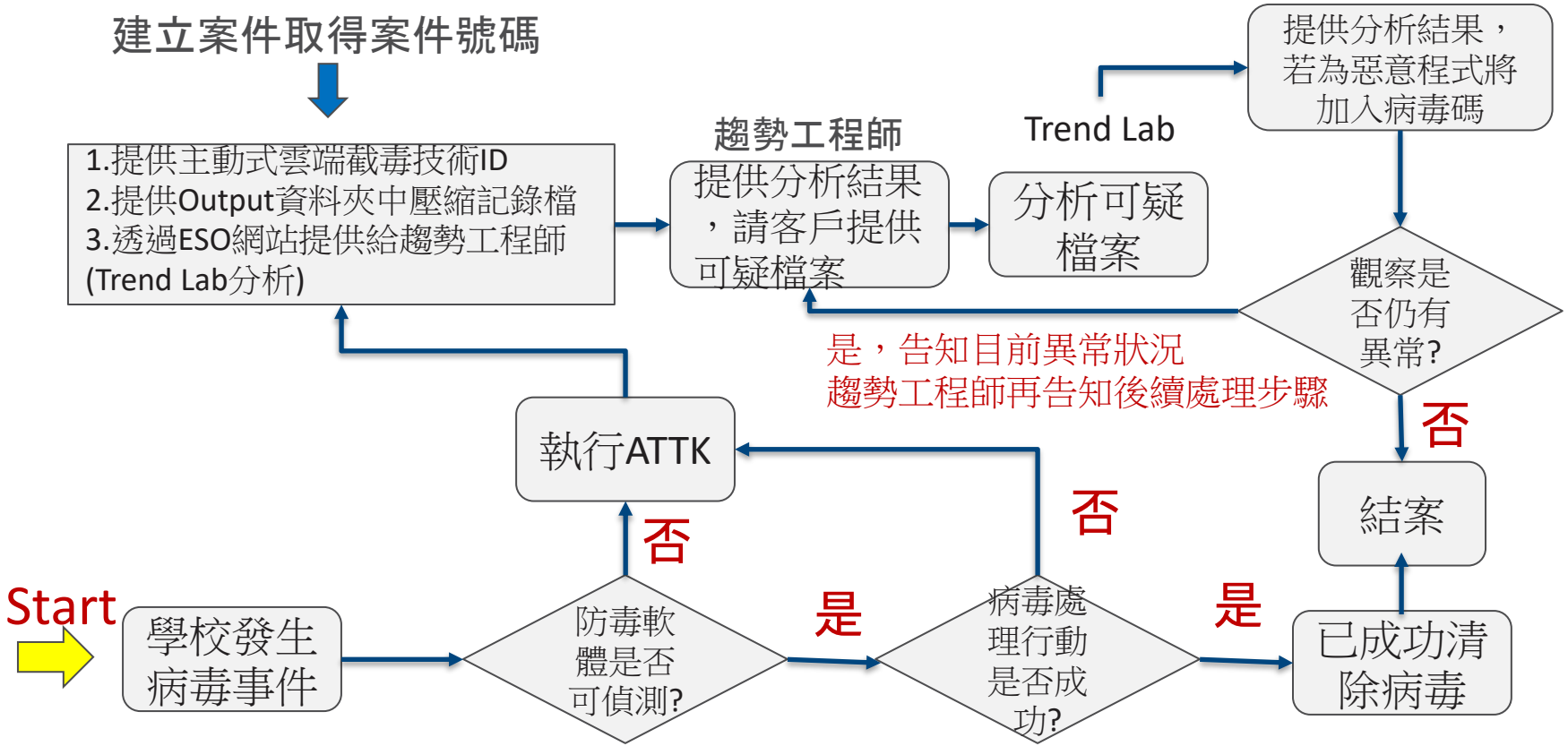
- 疑似中毒、暫時無法偵測之病毒(從防毒管理系統下載並執行ATTK)
- 將收集的病毒樣本回傳至趨勢科技分析，趨勢工程師會依據收集資訊分析結果，提供後續處理方式

2. 學校應了解自身狀況

- 分析感染原因：外來電腦、漏洞未補、未設密碼、上不良網站…
- 分析感染管道
- 制定學校安全政策、加強防禦、教育訓練

P.S. 合約內提供**無限次數專線電話支援**與防毒管理系統之線上諮詢服務。

病毒處理流程總覽



病毒處理流程細項介紹 – 判定是否需要執行工具(1/2)

病毒處理步驟:

步驟1. 學校反應病毒問題

→ 趨勢客服會協助確認病毒問題

步驟2. 客服會確認是否趨勢的防毒軟體可以偵測到 ?

- 是: 請執行步驟3
- 否: 請執行步驟5

步驟3. 客服會確認毒軟體執行病毒處理行動是否成功?

- 是: 請執行步驟4
- 否: 請執行步驟5

病毒處理流程細項介紹 – 判定是否需要執行工具(2/2)

步驟4. 與學校說明，趨勢防毒軟體已將病毒成功清除

========== 結束 ==========

病毒處理流程細項介紹－如何使用執行工具(ATTK)

步驟5. 請到ESO入口網站https://eso.ntpc.edu.tw（支援SSO）
客戶專屬>下載ATTK
依照下列步驟執行此工具:

PS. 此工具會不定期更新，建議每次到客戶端之前，可以先行下載當時最新版本!!

(1) 依據環

- 可上網的電腦（32位元）

  可上網的電腦（64位元）

- 無法上網的電腦（32位元）

  無法上網的電腦（64位元）

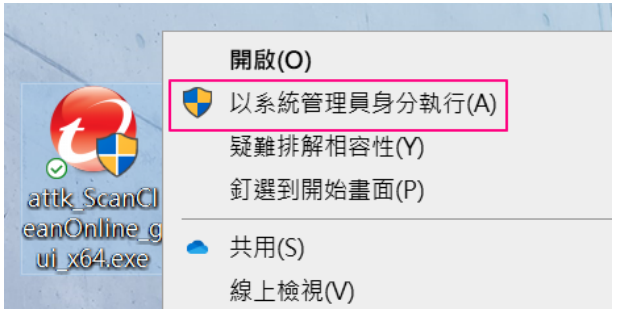
(2) 使用滑鼠點兩下attk_ScanXXX.exe ,程式會開始收集病毒相關資訊,執行收集資訊期間會出現以下視窗, **請勿**將其關閉

ATTK 執行步驟

1. 將下載完成的attk_ScanCleanXXX_XXX.exe放置於要收集的電腦上。

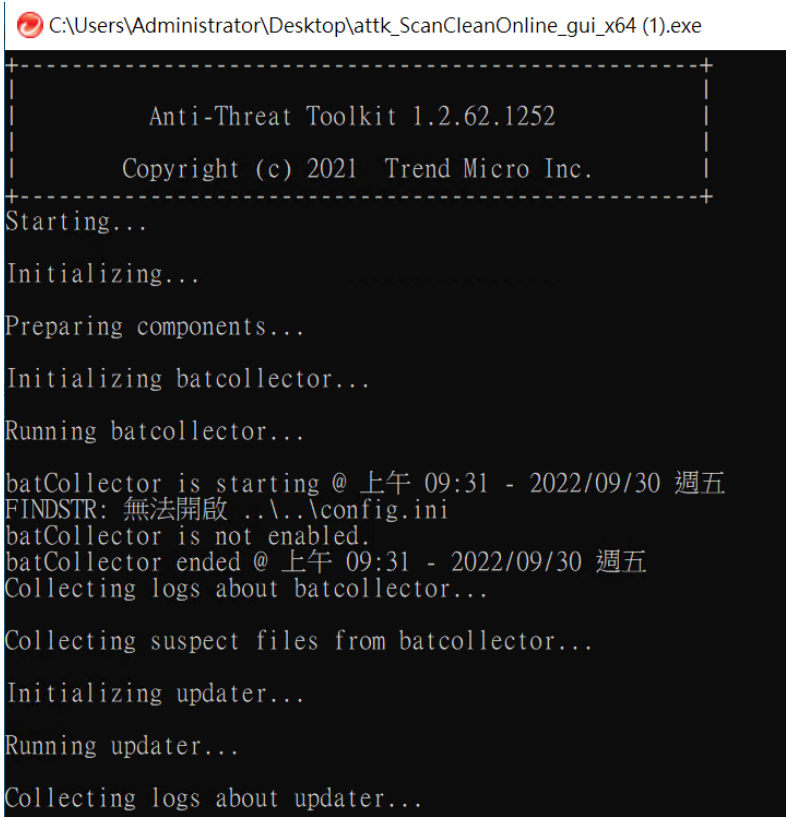
← 依據環境下載適合的程式

2. 請點選執行attk_ScanCleanOnline_gui_x64.exe ，請於點attk_ScanCleanOnline_gui_x64.exe選滑鼠右鍵，點選以系統管理員身分執行。



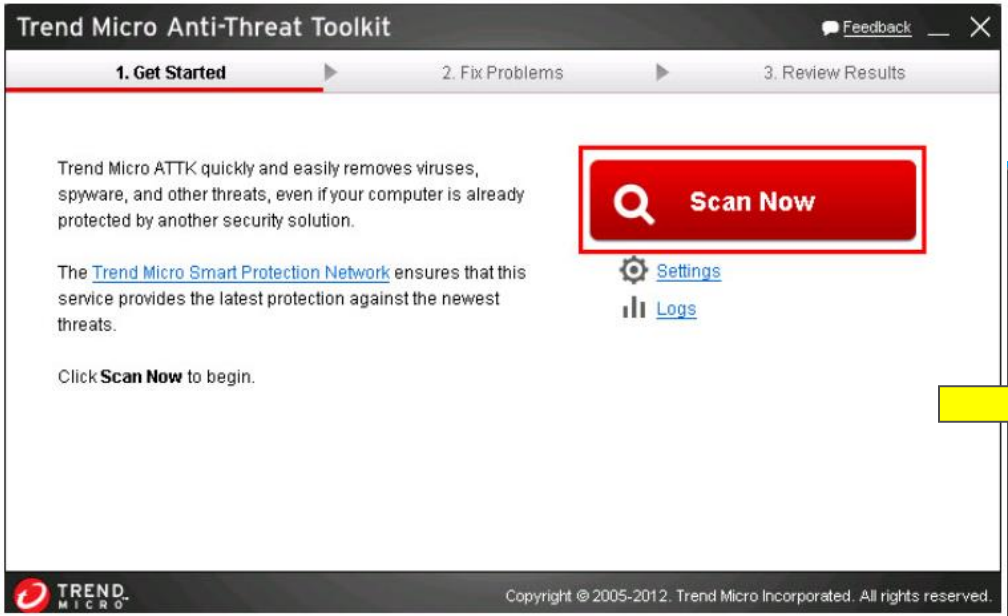
ATTK執行步驟

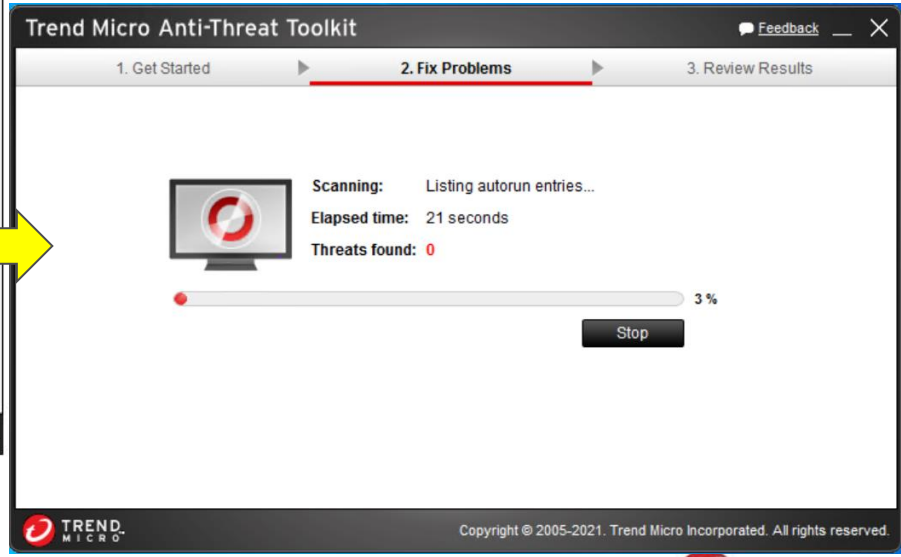
3. 這時候會出現一個命令提示字元模式的畫面，請不要關閉這個視窗。



ATTK執行步驟

4. 出現TrendMicro AntiThreat Toolkit的視窗，請點選【Scan Now】開始進行掃描。

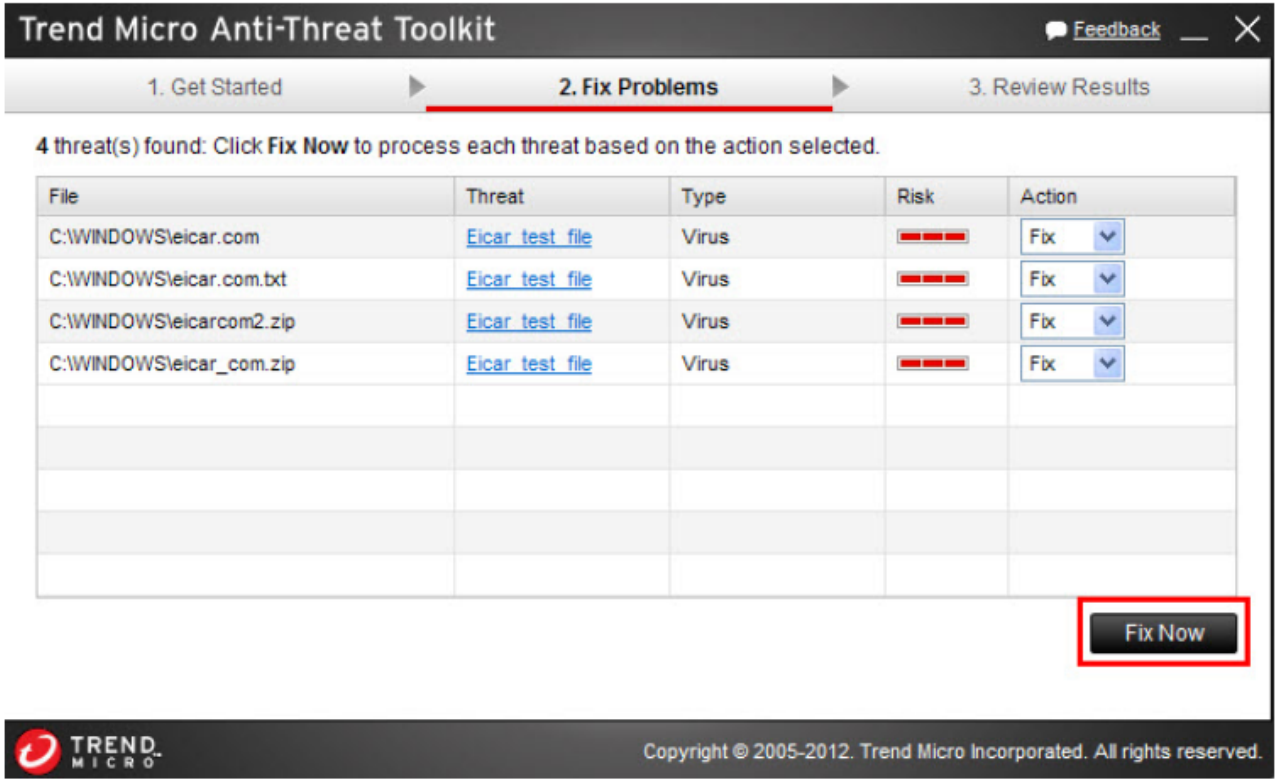




掃瞄可能會花費一些時間，工具將會列出掃描電腦時所找到的安全威脅。

ATTK執行步驟

5. 點選【Fix Now】來清除這些安全威脅。



ATTK執行步驟

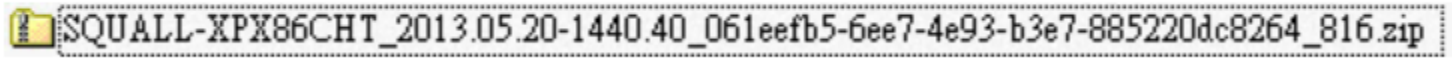
6. 清除完成後，可以點選右上方【X】結束 AntiThreat Toolkit。

ATTK執行步驟

7. 結束後會出現一個網頁視窗，顯示一個暫時ID號碼。

ATTK執行步驟

8.在工具執行時所產生的同名資料夾(TrendMicro AntiThreat Toolkit)中，找到Output資料夾，裡面會有一個壓縮的記錄檔。



9.請將主動式雲端截毒技術ID號碼和Output裡的壓縮記錄檔一起提供給趨勢科技技術支援中心。

病毒處理流程細項介紹 – 如何提交ATTK檔案

步驟6.

6.1 請透過線上處理案件系將主動式雲端截毒技術ID、壓縮檔提交給趨勢科技工程師

請注意: 1. 請務必依照下列註明事項填寫

2. 僅適用於新北教網指定的學校提交病毒案件使用

- 部門名稱: 請填寫學校名稱
- 聯絡人姓名/聯絡人電子信箱/聯絡電話: 請填寫負責老師聯絡資訊

  E-mail & 電話請務必填寫正確, 以便於之後tool 的提供以及後續的聯絡
- 問題描述: 請儘量寫清楚所遇到的問題,以避免因為資訊不清楚,

  造成信件往返多次,延遲病毒分析速度

(請務必依照指定格式填寫)

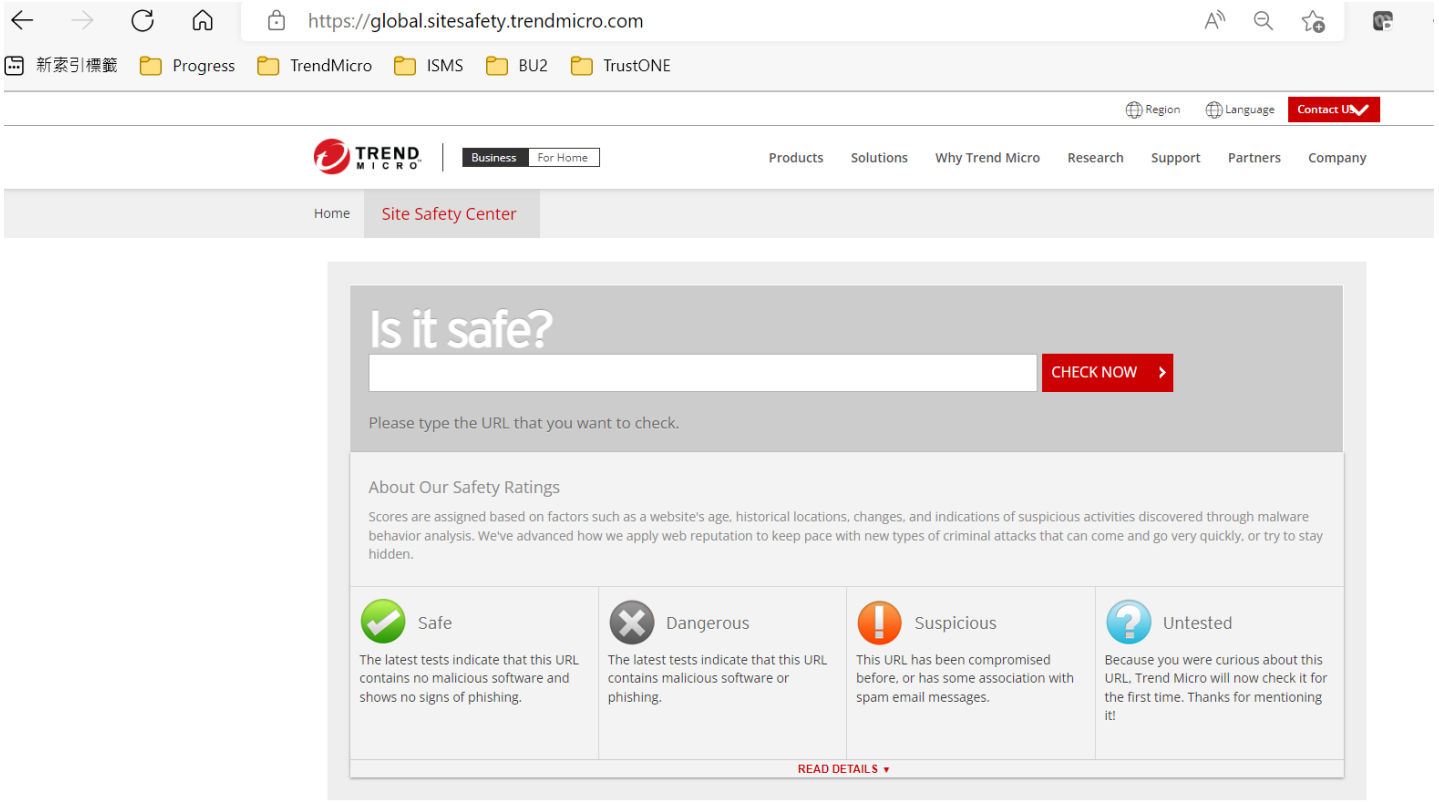
病毒處理流程細項介紹－如何提交ATTK檔案

病毒處理流程細項介紹－如何提交病毒樣本

病毒處理流程細項介紹 – 如何提交郵件分析

病毒處理流程細項介紹－如何提交網頁類別分析-1

病毒處理流程細項介紹 – 如何提交網頁類別分析-2



病毒處理流程細項介紹－如何提交病毒資訊需求

病毒處理流程細項介紹－如何提交其他病毒問題

病毒處理流程細項介紹 – 分析&提供處理步驟(1)

步驟7. 趨勢科技工程師根據學校提供的資訊以及log，提供給TrendLab分析，分析後會透過E-mail請客戶提供可疑檔案

步驟8. TrendLab分析後，趨勢科技工程師提供分析結果，若為惡意程式將加入病毒碼

病毒處理流程細項介紹－分析&提供處理步驟(2)

步驟9. 學校觀察是否仍有異常

- 是: 請執行步驟10
- 否: 請執行步驟11

步驟10. 學校告知目前異常狀況為何?趨勢工程師會再告知後續處理步驟，回到步驟7繼續執行

步驟11. 當趨勢科技工程師收到回覆無異常的信後，會將此案件結案

技術支援專線及專屬線上服務

- 各校資訊人員如需諮詢病毒、產品問題，
  請撥技術支援專線: 02-2377-2323#1
- 教研中心防毒窗口如需諮詢病毒、產品問題，
  請撥技術支援專線: 03-3019399#3
- ESO 線上服務申請:https://eso.ntpc.edu.tw

其他說明-用戶端安裝

1.確認電腦的命名規則：

(Domain Name - pc name)

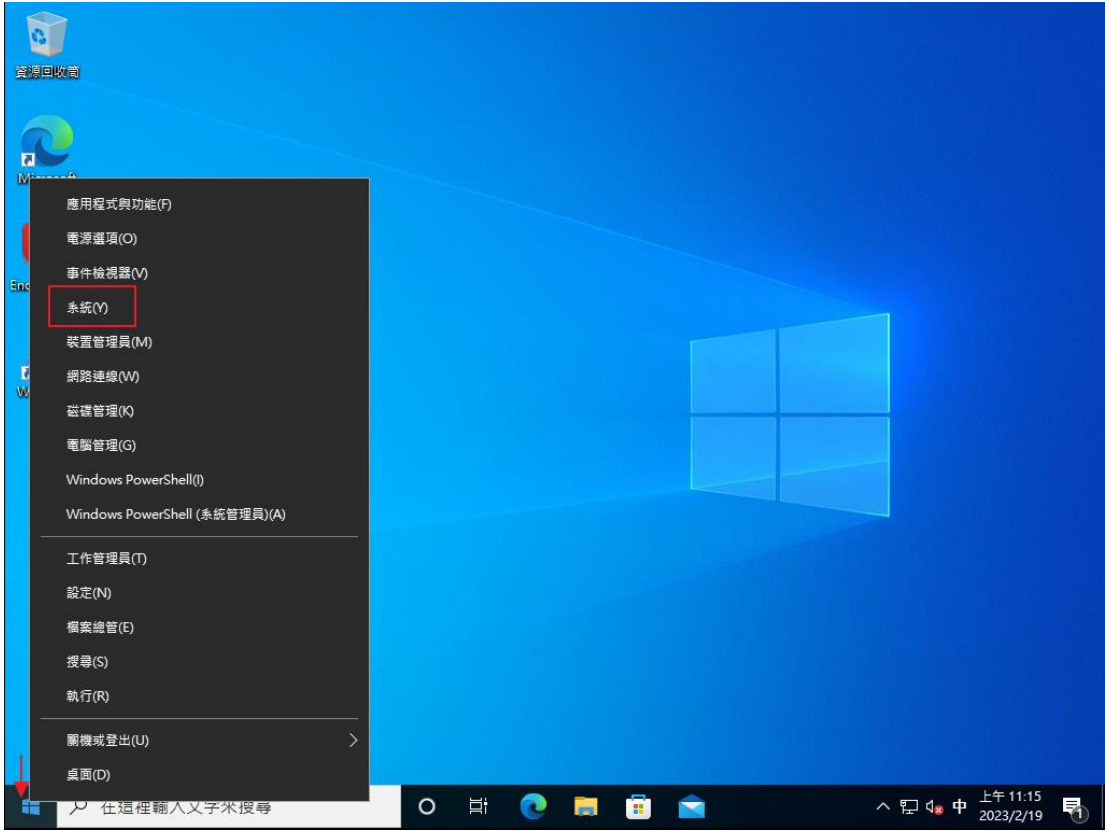
Domian name < -學校名稱

例:大觀國中英文縮寫為

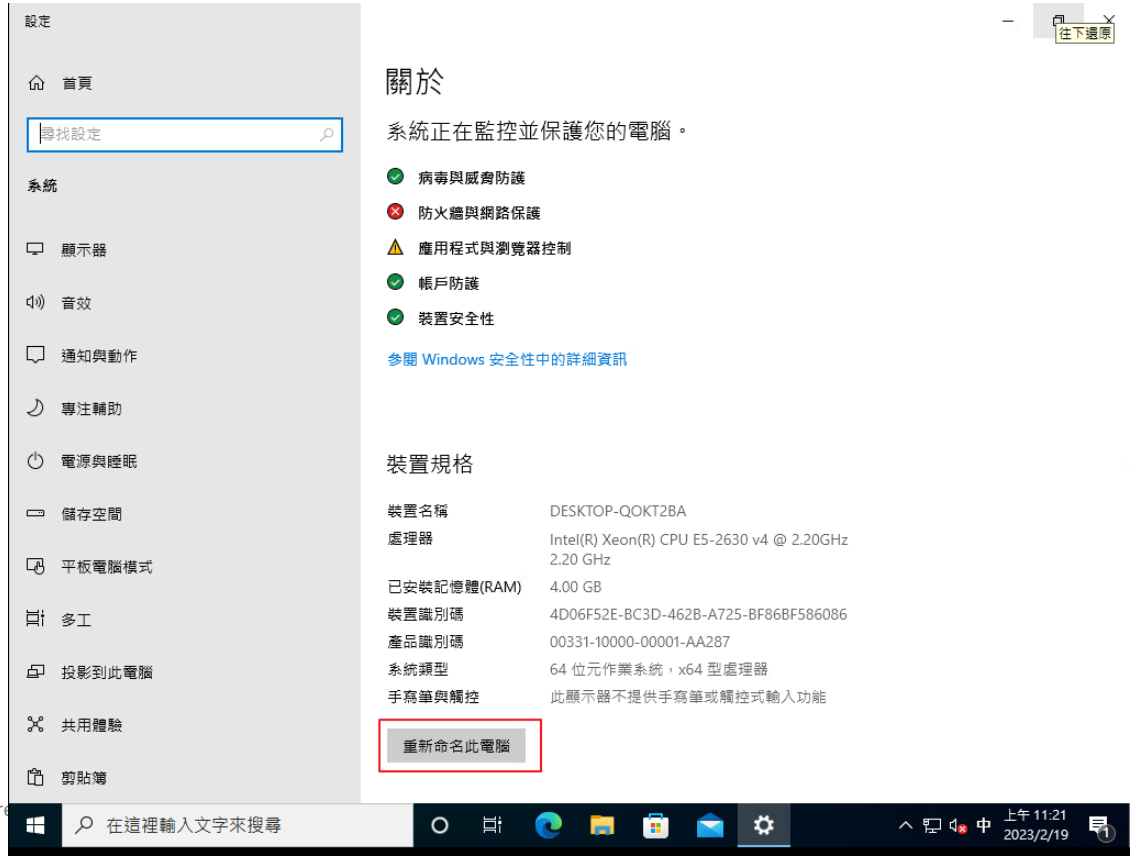
tkjhs。所以命名為:tkjhs-XXX

如何修改/確認電腦的名稱-Windows 10

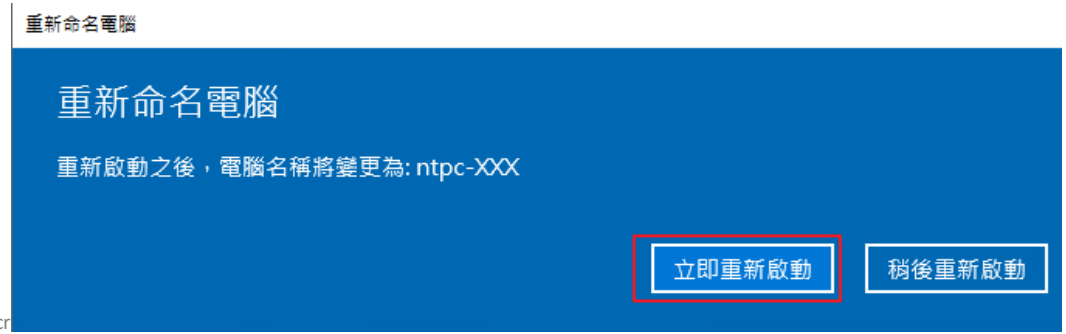
- 左下角開始圖示按右鍵點[系統]



- 點[重新命名此電腦]



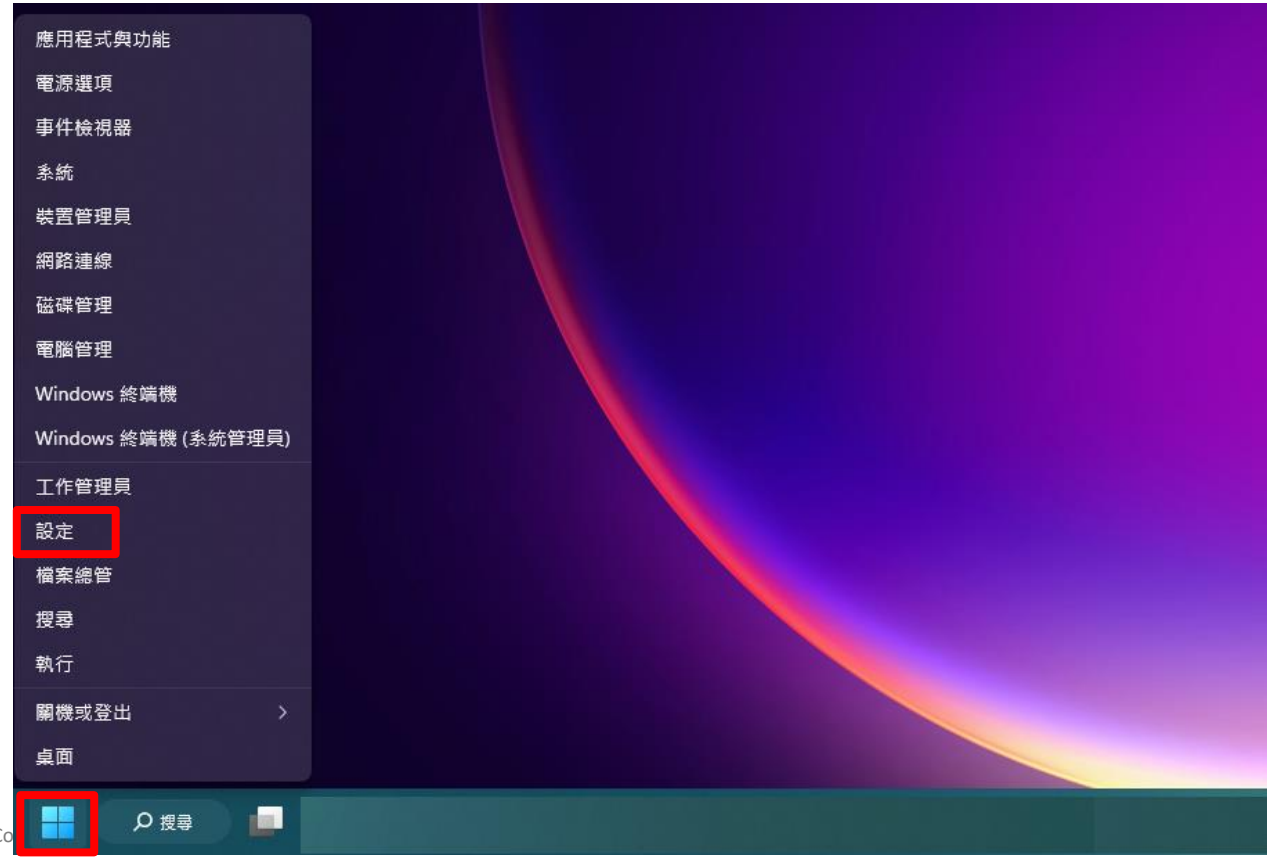
- 輸入電腦名稱(依據電腦的命名規則)，按[下一步]，確認名稱後，按[重新啟動電腦]後即完成。



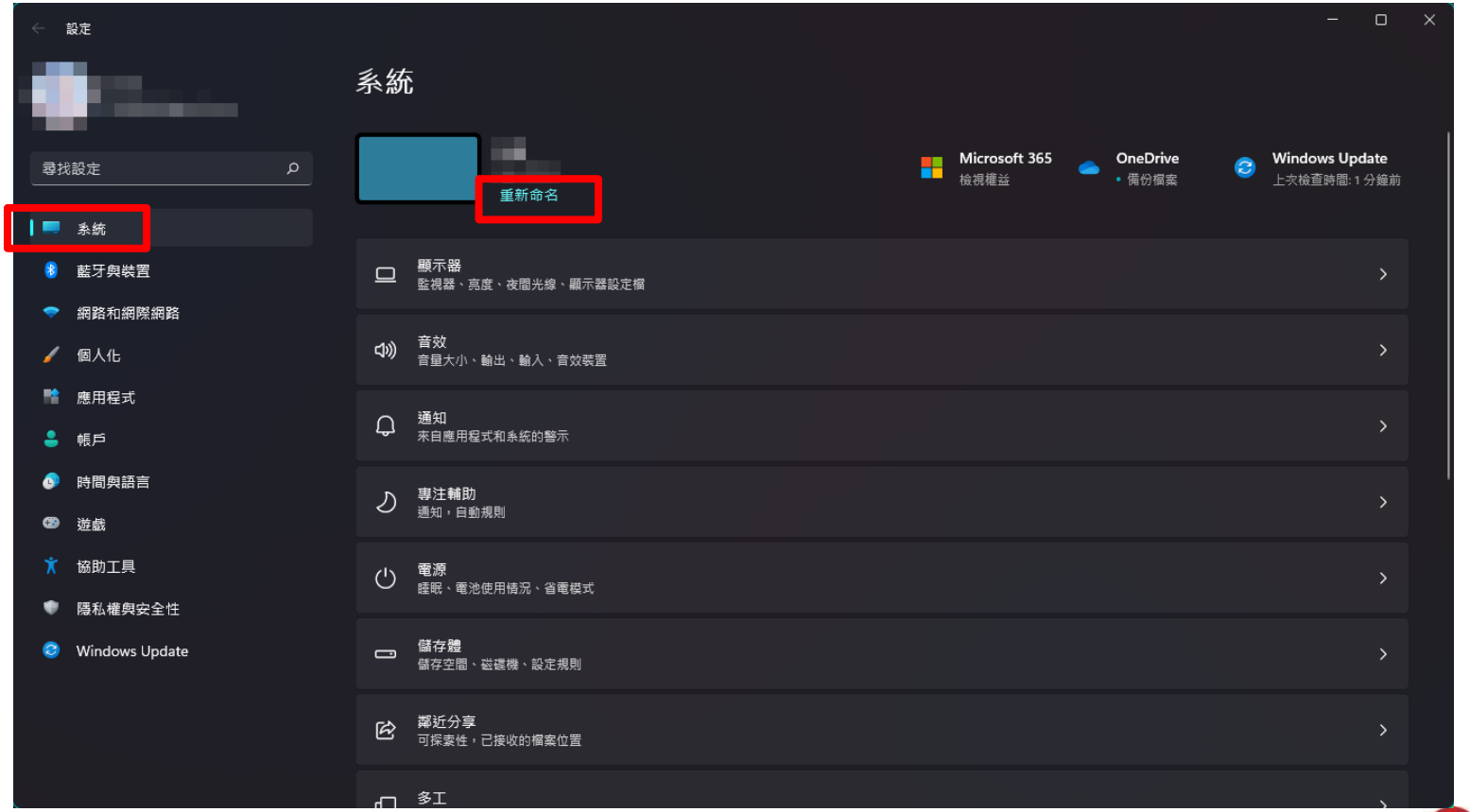
- 左下角開始圖示按右鍵點[系統]，再次確認裝置名稱是否正確。

如何修改/確認電腦的名稱-Windows 11

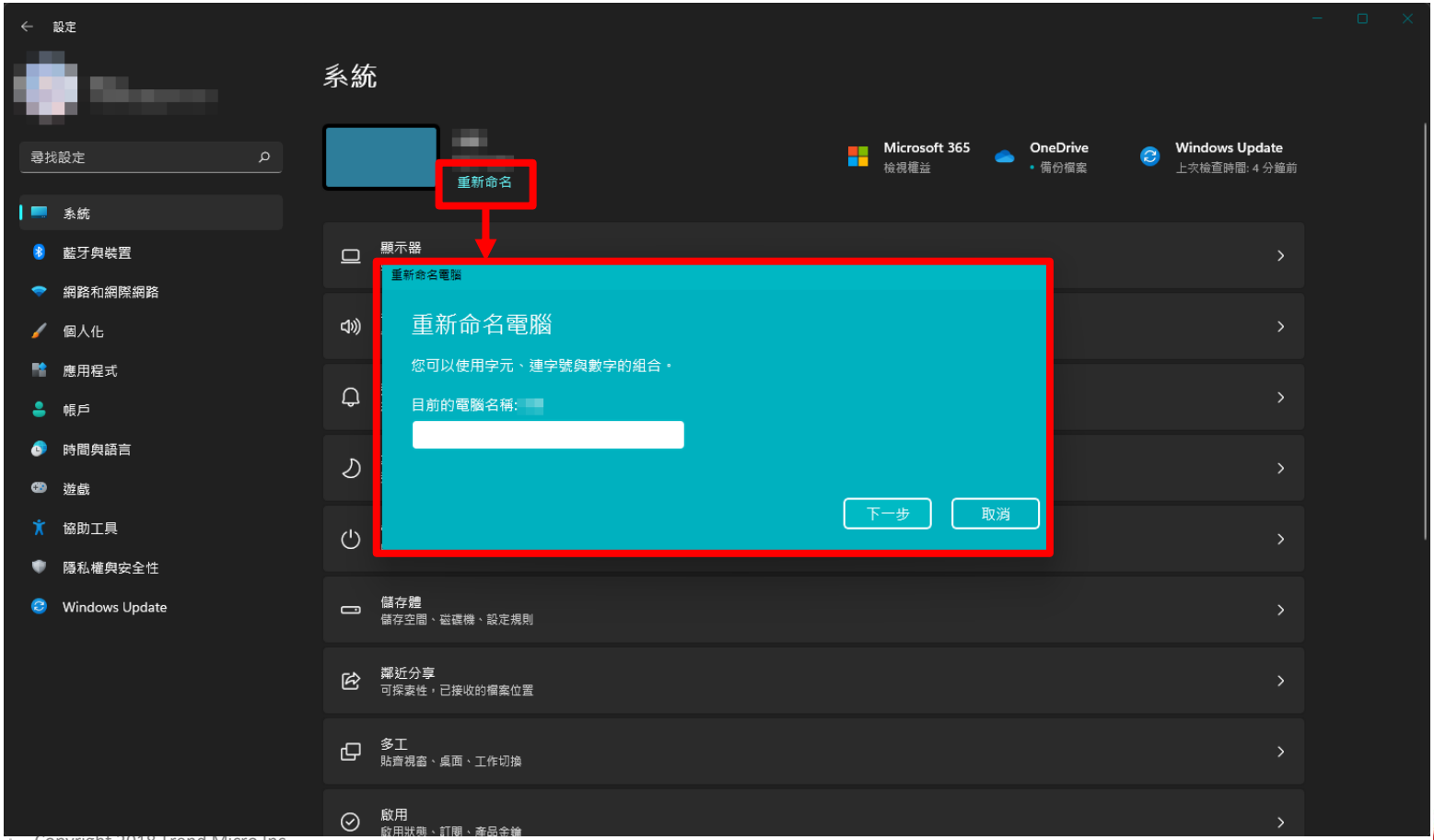
- 左下角開始圖示按右鍵點[設定]



- 選擇[系統]頁面，點擊上方的[重新命名]。



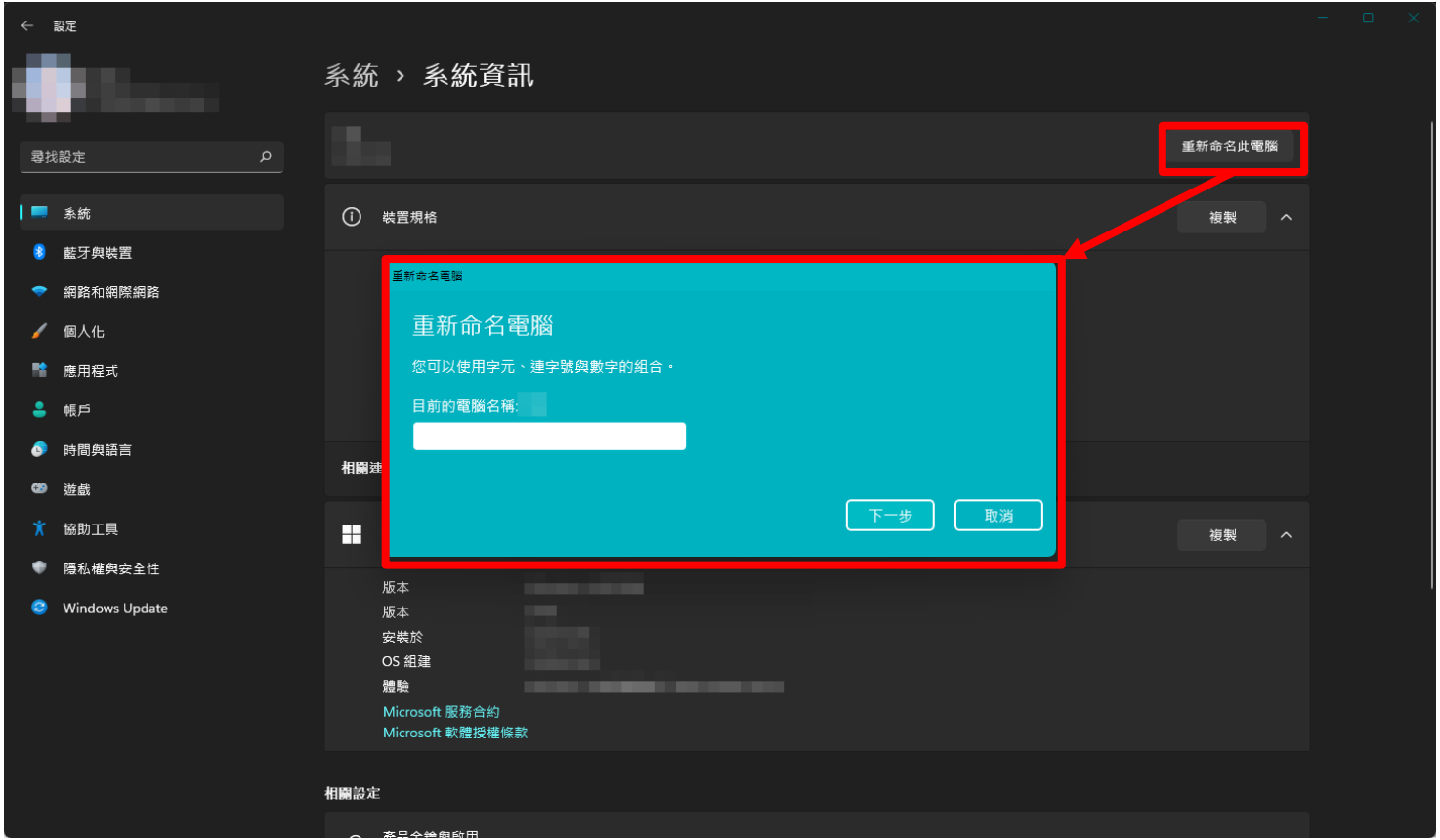
- 輸入名稱後，點選[下一步]。



- 或是在[系統]頁面中，選擇最下方的[系統資訊]。

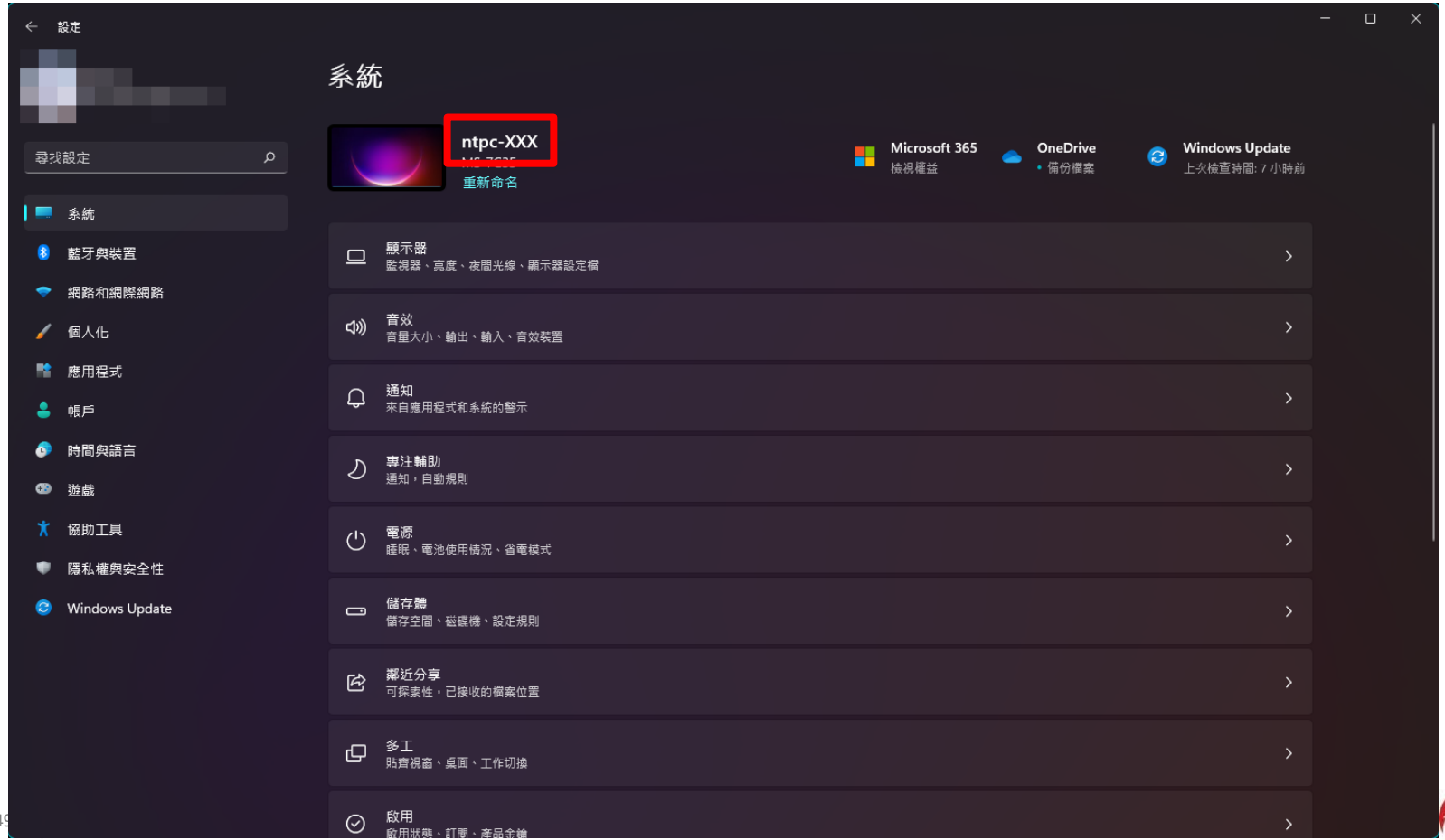
- [系統資訊]的頁面右上方， 點擊[重新命名此電腦的]。

- 輸入名稱後，點選[下一步]。



- 輸入電腦名稱(依據電腦的命名規則)，按[下一步]，確認名稱後，按[立即重新啟動]後即完成。

- 左下角開始圖示按右鍵點[設定]，再次確認裝置名稱是否正確。



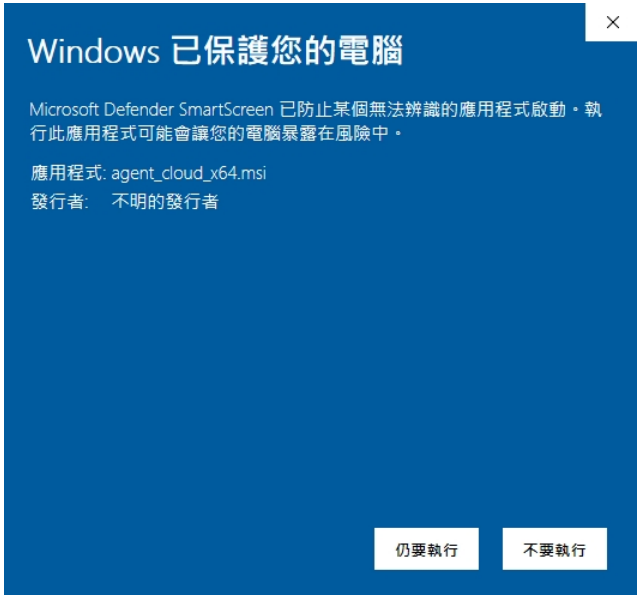
2. 用戶端下載位置

https://osce.ntpc.edu.tw/

無需輸入密碼,點選以下的安裝程式.選擇自己的版本進行下載

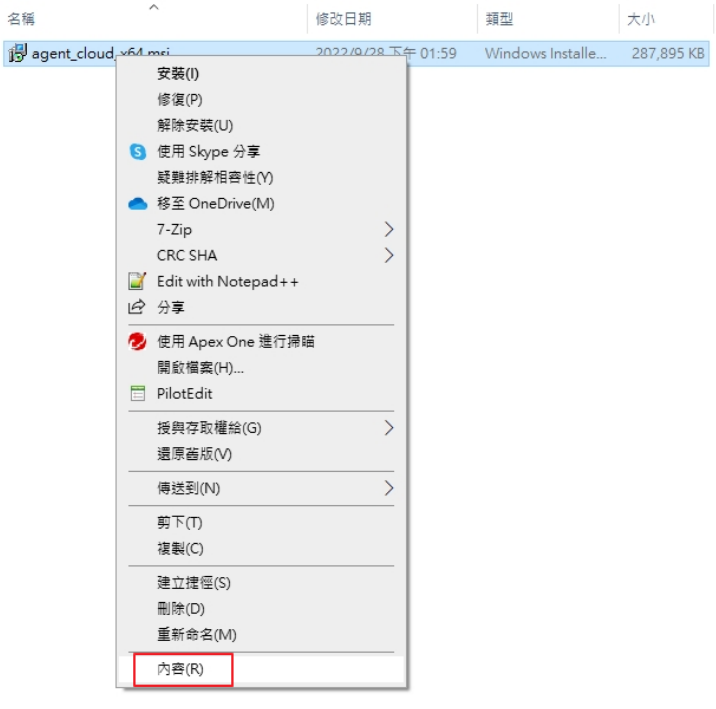
用戶端程式安裝方式- Internal Web Page(1)

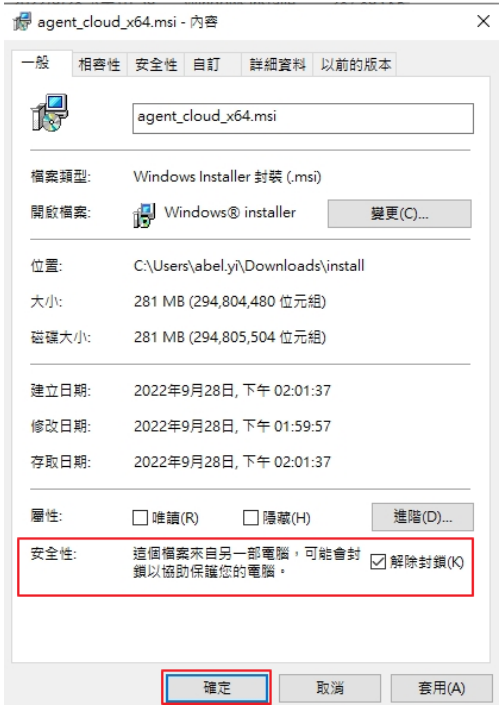
3. 若直接執行 MSI 可能會出現此訊息，點選「其他資訊」>「仍要執行」。



用戶端程式安裝方式- Internal Web Page(2)

4. 在執行 MSI 前，確認檔案是否有安全性限制，如果有請先解除，可以點選「內容」>「解除封鎖」。



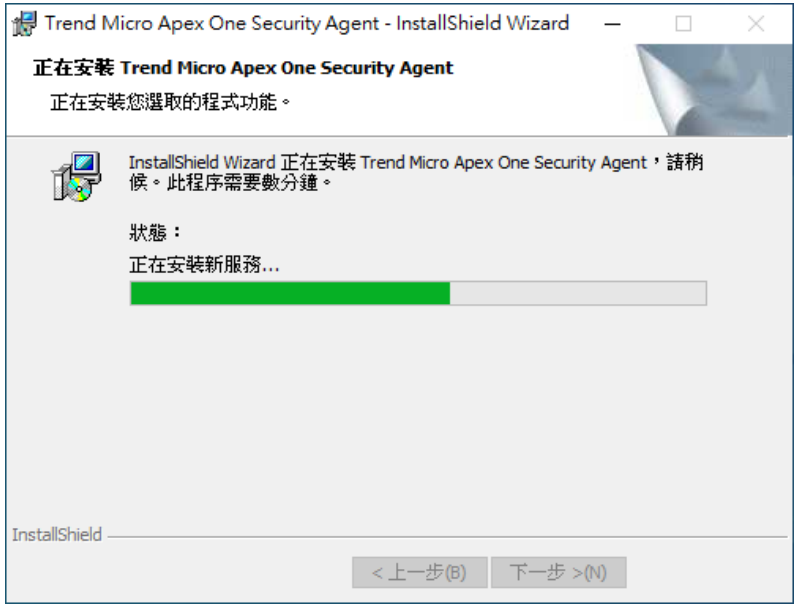


用戶端程式安裝方式- Internal Web Page(3)

5. 點選「下一步」

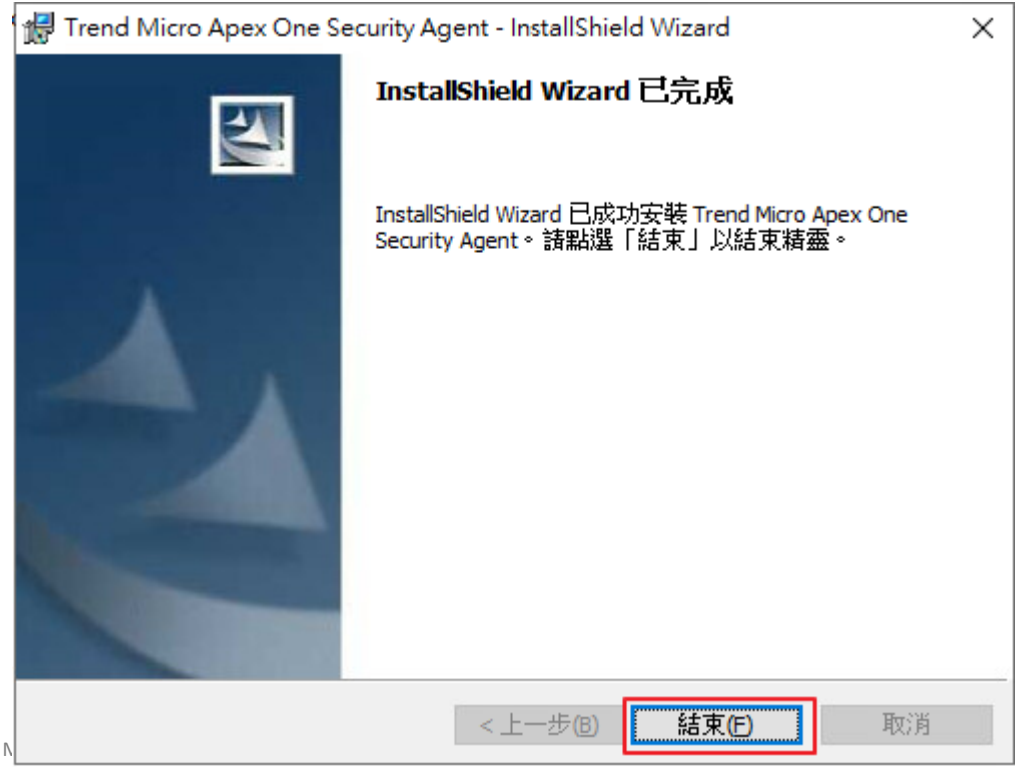
用戶端程式安裝方式- Internal Web Page(4)

6. 安裝過程畫面



用戶端程式安裝方式- Internal Web Page(5)

7. 安裝完成，點選「結束」



用戶端程式安裝方式-Internal Web Page(6)

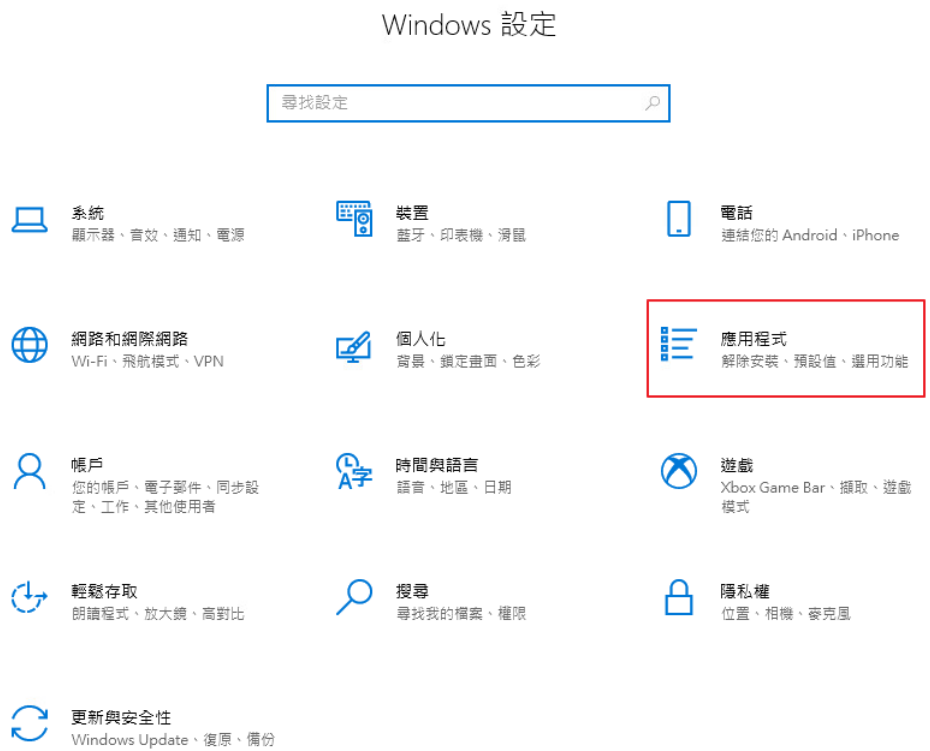
8. 如果警告跳出視窗，可以不用立即重新啟動電腦，在方便重啟的時間點進行電腦重新開機即可。

用戶端程式安裝方式- Internal Web Page(7)

9. 執行 ApexOne 用戶端安裝程式後，程式將自行安裝且連線至教網中心防毒主機
10. 安裝完成確認右下角出現 ApexOne 用戶端圖示

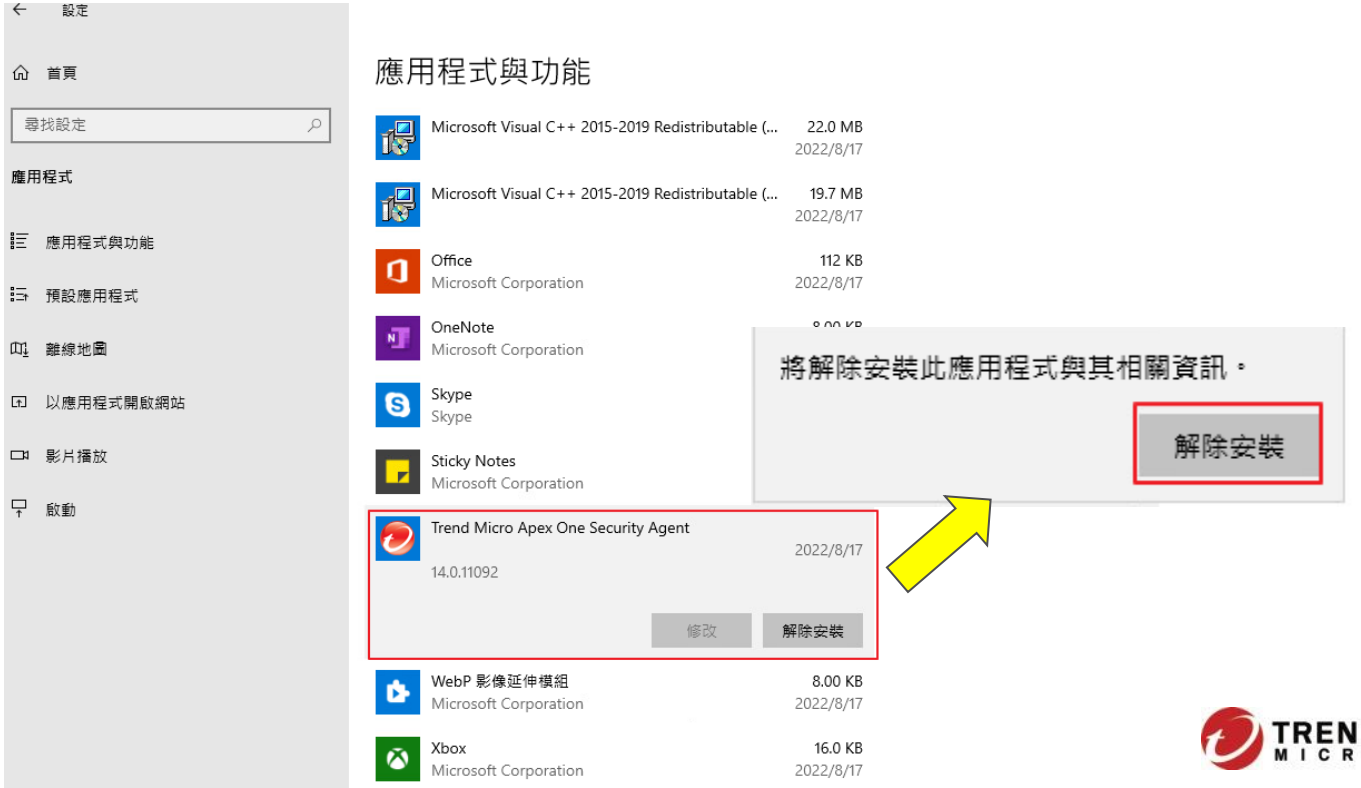
用戶端程式移除方式-(1)

1. 設定 > 應用程式（以Windows10為例）



用戶端程式移除方式-(2)

2. 應用程式與功能中找到Trend Micro Apex One Security Agent，點「解除安裝」



用戶端程式移除方式-(3)

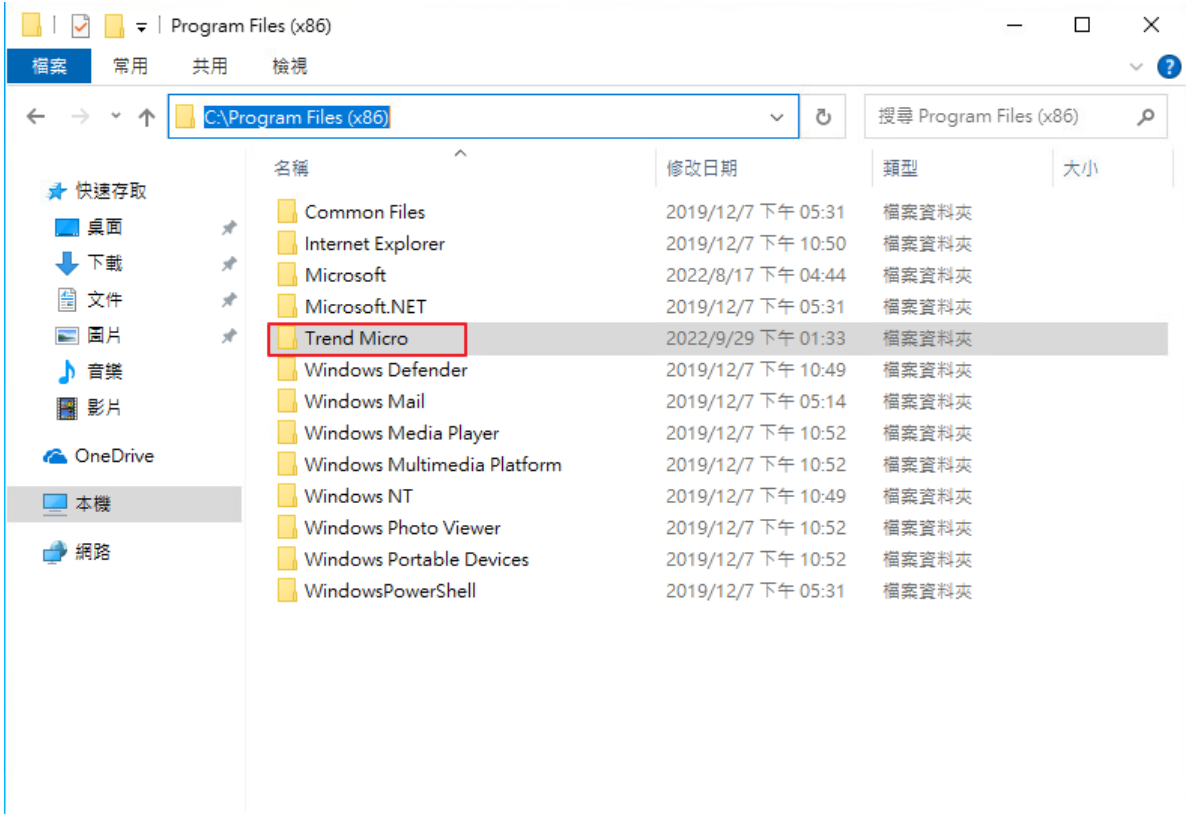
3. 輸入解除安裝密碼，點「確定」。(請洽各校資訊組長索取移除密碼)

用戶端程式移除方式-(4)

4. 移除完成，跳出訊息視窗，點「確定」

用戶端程式移除方式-(5)

5. 電腦重開機後，手動刪除C:\Program Files(x86)\Trend Micro資料夾



勒索軟體與行動裝置安全

勒索軟體防護與解密工具

勒索病毒肆虐?

新聞

麗臺遭遇勒索軟體攻擊，本週第二起上市公司發布資安事件重大訊息

本週國內上市公司接連傳出遭駭客攻擊，繼雄獅旅遊之後，繪圖卡研發製造廠麗臺科技也發布相關公告，目前該公司已說明是遭勒索軟體攻擊，受影響系統皆陸續回覆運作，這次事件對生產及營運並不會帶來重大影響

文/ 羅正漢 | 2022-12-02 發表

讚 155 分享

本資料由 (上市公司) 2465 麗臺 公司提供

序號	1	發言日期	111/12/01	發言時間	16:58:08
發言人	楊智昆	發言人職稱	董事長特別助理	發言人電話	02-82265800-201
主旨	本公司遭駭客網路攻擊				
符合條款	第 26 款	事實發生日	111/12/01		
說明	1.事實發生日:111/12/01 2.發生緣由:麗臺科技遭受駭客網路攻擊 3.處理過程:本公司資安團隊於第一時間啟動防禦機制及備援作業，並與外部資訊技術專業人員共同合作處理，並將所監測到的異常狀況，通報予政府相關執法部門，並保持密切聯繫。 4.預計可能損失或影響:目前對本公司生產、銷售及日常營運無重大影響。 5.可能獲得保險理賠之金額:不適用。 6.改善情形及未來因應措施:本公司已於第一時間啟動資安防禦，並對網路攻擊進行清查，受到影響的內部資訊系統均已陸續回復運作，本				

勒索病毒肆虐?

新聞

華碩子公司NAS設備遭DeadBolt勒索軟體攻擊

華碩集團旗下華芸科技（Asustor）NAS設備遭DeadBolt勒索軟體攻擊，官方發出公告，呼籲遭攻擊用戶立即拔除乙太網路連線，長按電源鍵關閉NAS，同時不要啟動NAS以免資料被刪除，並聯絡華芸提供技術支援

文/ 林妍溱 | 2022-02-23 發表

讚 326 分享

2月25日補充更新資訊

對於這次事件的受害用戶，華芸科技在25日（週五）12時於該公司粉絲專頁發布新的公告，說明DeadBolt勒索軟體遇害的解決方法，供用戶依照相關步驟與狀況來排除被勒索的情形。文⊙iThome資安主編羅正漢

勒索軟體攻擊新聞事件不斷發生

ETtoday新聞雲

傳付3億贖身！Garmin電腦遭駭客綁架 關鍵「2檔案」曝光

... 遭勒索軟體「綁架」，就連Garmin台灣分公司也受害，網路中斷4天，直到7

奇摩股市

不只鴻海！駭客入侵台灣逾10大企業 仁寶、研華遭勒索近10億

數位時代

宏碁遭駭客REvil勒索天價14億元！成微軟漏洞受害者，官方

蘋果日報

廣達被駭遭勒索14億！ Apple重要產品設計圖驚傳外洩｜ 蘋果 ...

去年11月，筆電代工大廠仁寶與研華科技皆傳出遭到駭客勒索，金額達10億元，仁寶董事長許勝雄後續回應，證實有發現駭客存在但並未支付贖金 ...

2 週前

勒索軟體演進

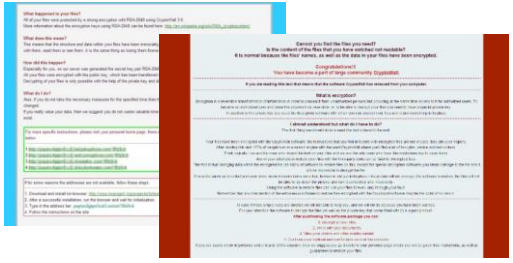
2006. TROJ_CRYZIP

2012. Reveton

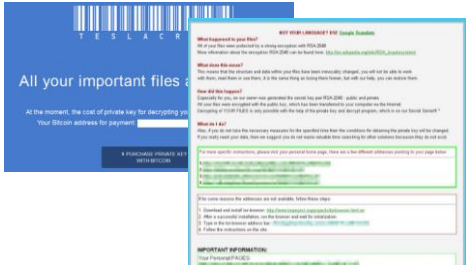
2013. CryptoLocker

2013 ~ . TorrentLocker Family

2014 ~ . CryptoWall Family



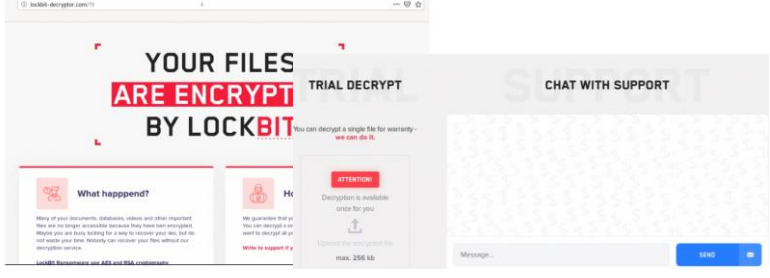
2015 ~ . TeslaCrypt Family



2017 ~ . WanaCry Family

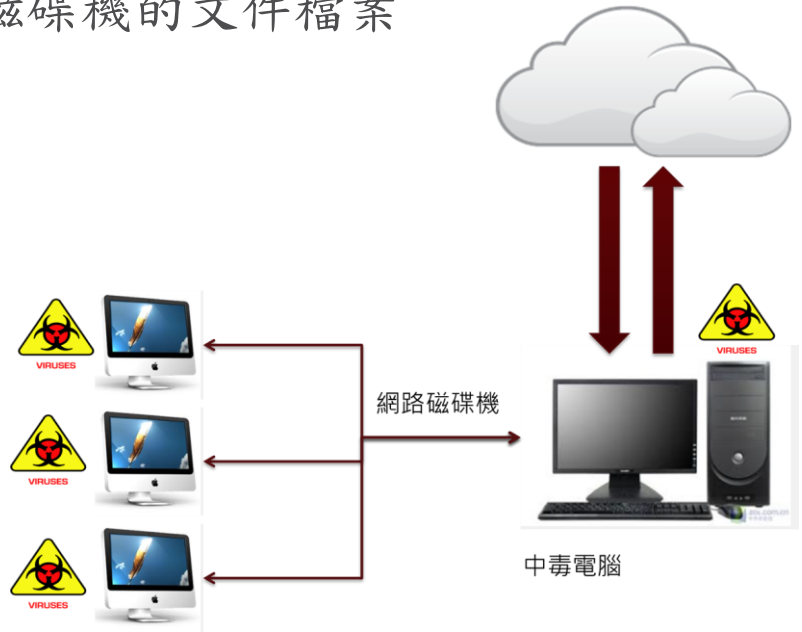
2020. Conti

2021~ . Lockbit



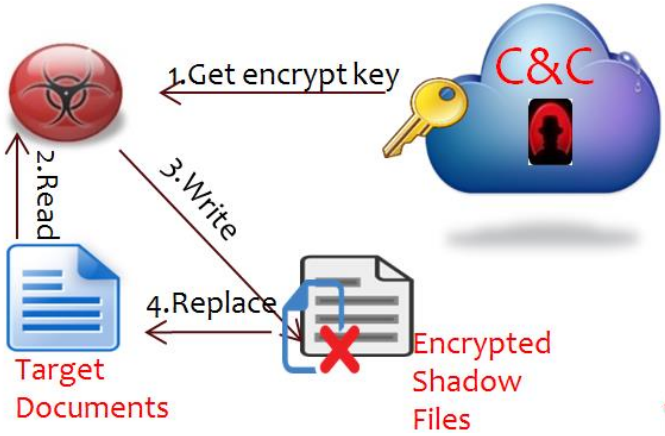
勒索軟體的特性：把你的檔案當作人質-加密

- 加密 電腦中“有寫入權限“文件檔案
- 加密 電腦中 包含所有網路磁碟機的文件檔案



勒索軟體的特性：文件無法自行解密

- 檔案是由AES / RSA 2048 加密演算法加密
- 一經加密即無法破解，除非取得金鑰

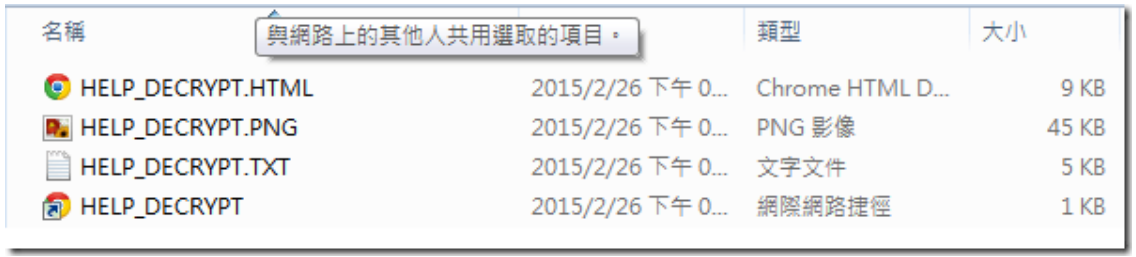


1

It changes entire file content

勒索軟體的特性：被加密文件將無法使用

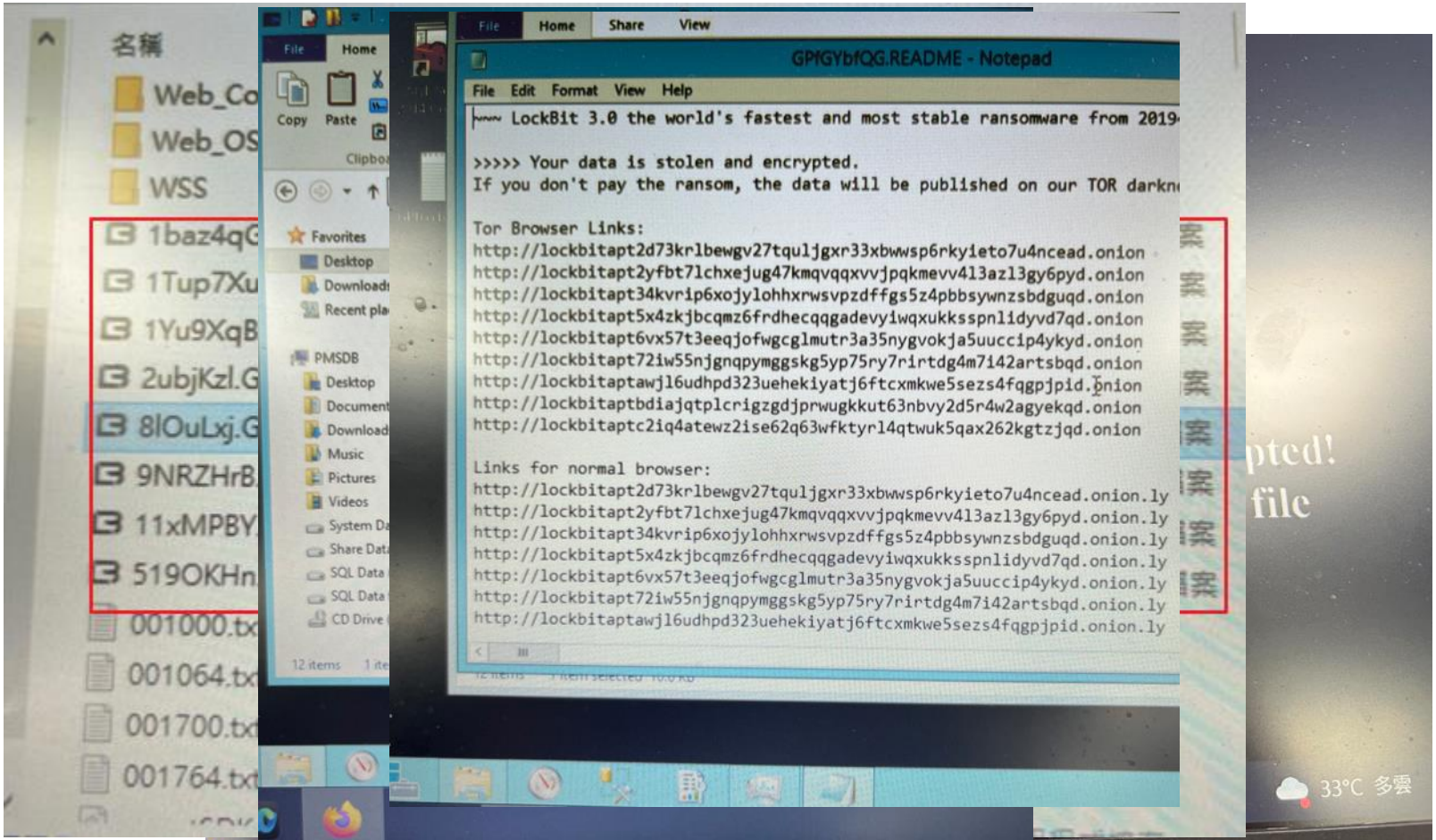
- 中了此類病毒後會優先攻擊文件、圖片、影音資料被加密，文件檔案會多一串 「encrypted、exx 、 micro、mp3 ……」的字眼
- 所有被加密檔案將無法使用



勒索軟體的特性：勒索付錢才給解密鑰匙

- 彈跳出勒索畫面要求支付贖金
- 使用Bitcoin交易
- 能復原靠運氣

實際案例畫面


名稱
Web_Co
Web_OS
WSS
1baz4qG
1Tup7Xu
1Yu9XqB
2ubjKzl.G
8lOuLxj.G
9NRZHrB
11xMPBY
519OKHn
001000.tx
001064.tx
001700.tx
001764.tx
File
Home
Copy
Paste
Favorites
Desktop
Recent pla
PMSDB
Desktop
Music
Pictures
Videos
12 items
File Home Share View
GPtGYbfQG.README - Notepad
File Edit Format View Help
LockBit 3.0 the world's fastest and most stable ransomware from 2019
>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darkn
Tor Browser Links:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyrl4qtwuk5qax262kgtzjqd.onion
Links for normal browser:
http://lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrip6xojylohhxrwsvpzdffgs5z4pbbsywnzsbdguqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frdhecqqgadevyiwqxukksspnlidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion.ly
http://lockbitapt72iw55njgnqpymggskg5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqgpjpid.onion.ly
pted!
file
33°C 多雲

勒索軟體的散播途徑

勒索軟體目前主要的攻擊途徑:

- 惡意郵件
  - 釣魚連結和惡意夾檔
- 網頁掛馬
  - 遭駭客入侵的網站
  - 惡意廣告
- 弱點攻擊
  - IE browser
  - Java /Flash
  - Adobe …

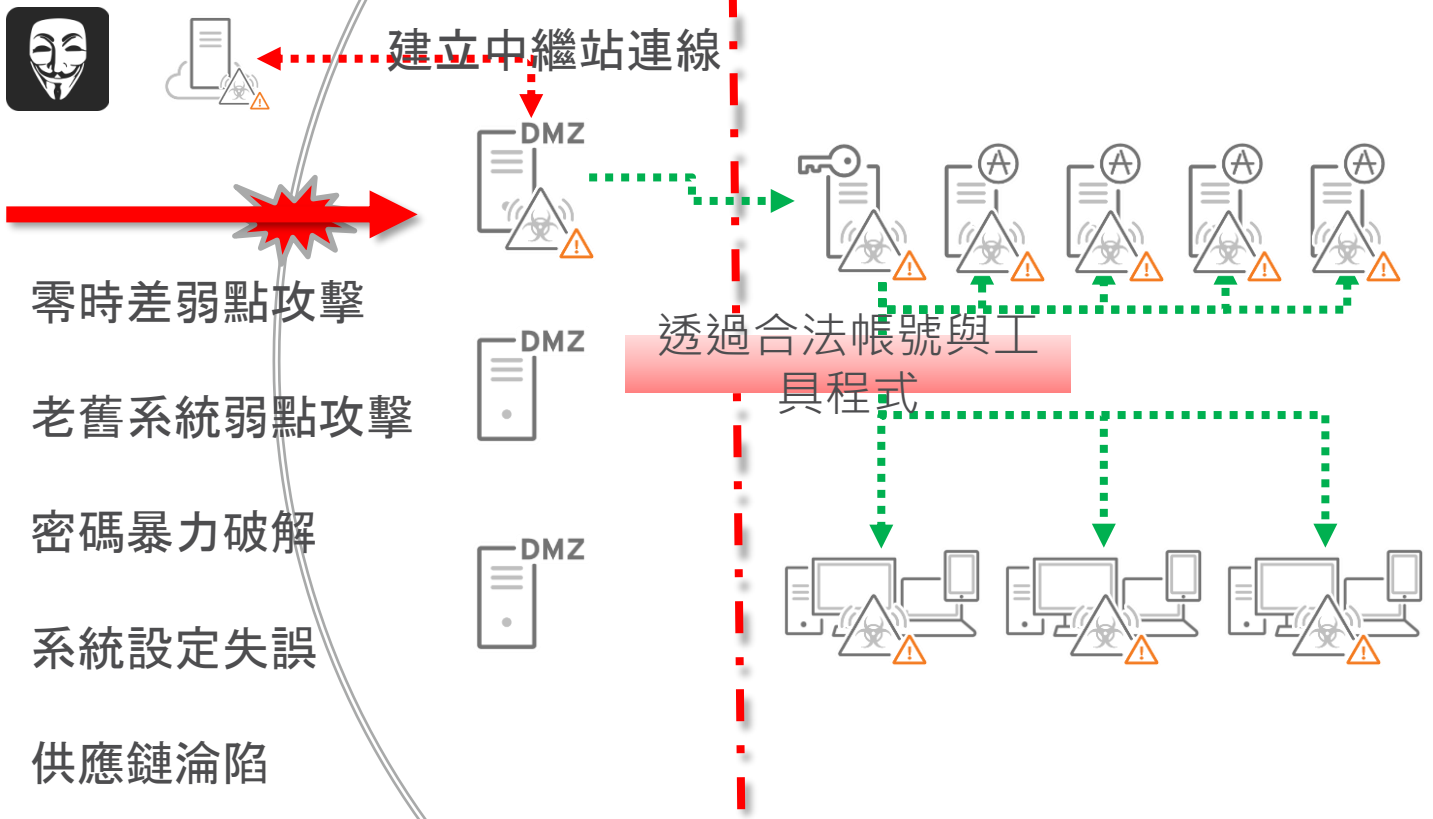
*User may encounter ransomware variants via **spam** or **malicious link**. Once installed, it limits access to the system and Show message prompts forcing users to **pay** for the Ransom*

勒索病毒威脅轉變

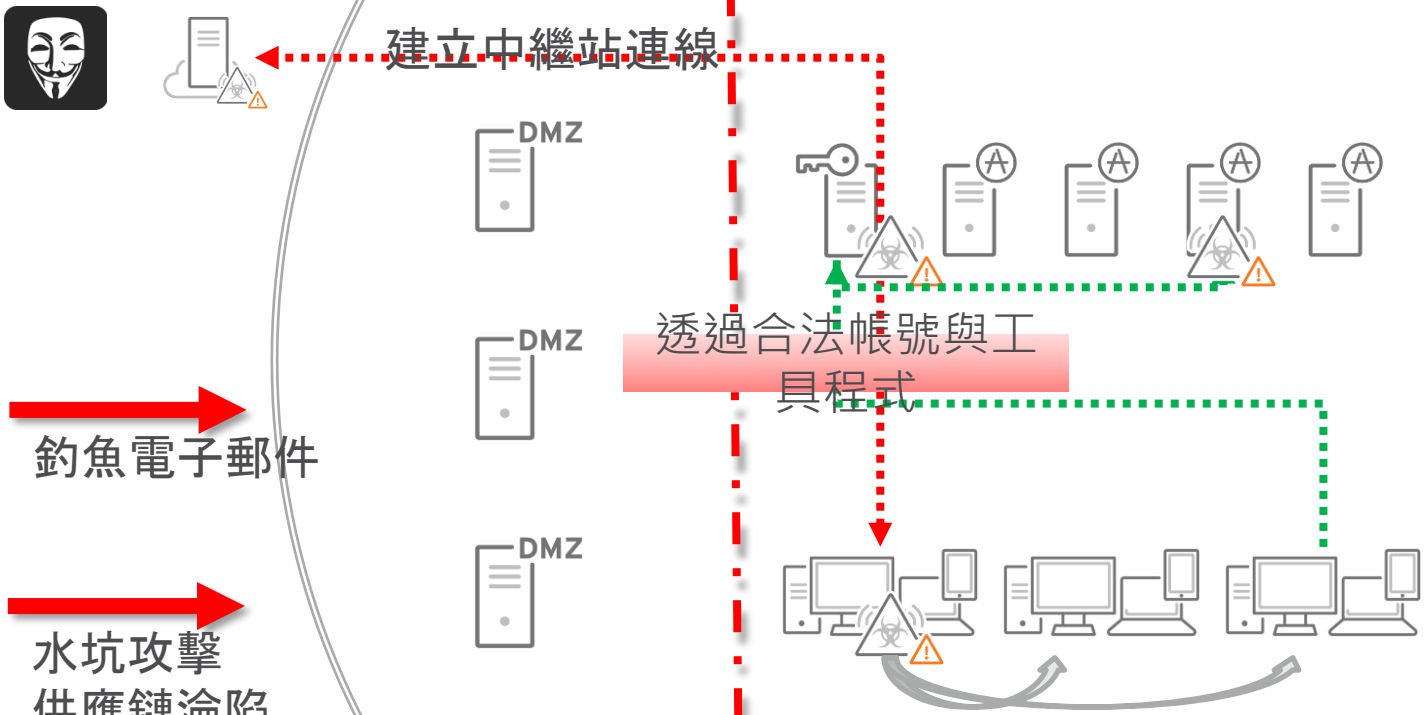
- 目標式勒索(Target Ransomware)的攻擊持續增加
  採APT 攻擊手法，大量加密PC/伺服器

攻擊流程手法案例分析(某公司)

近年常見駭客攻擊手法


建立中繼站連線
DMZ
DMZ
DMZ
零時差弱點攻擊
老舊系統弱點攻擊
密碼暴力破解
系統設定失誤
供應鏈淪陷
透過合法帳號與工具程式

近年常見駭客攻擊手法



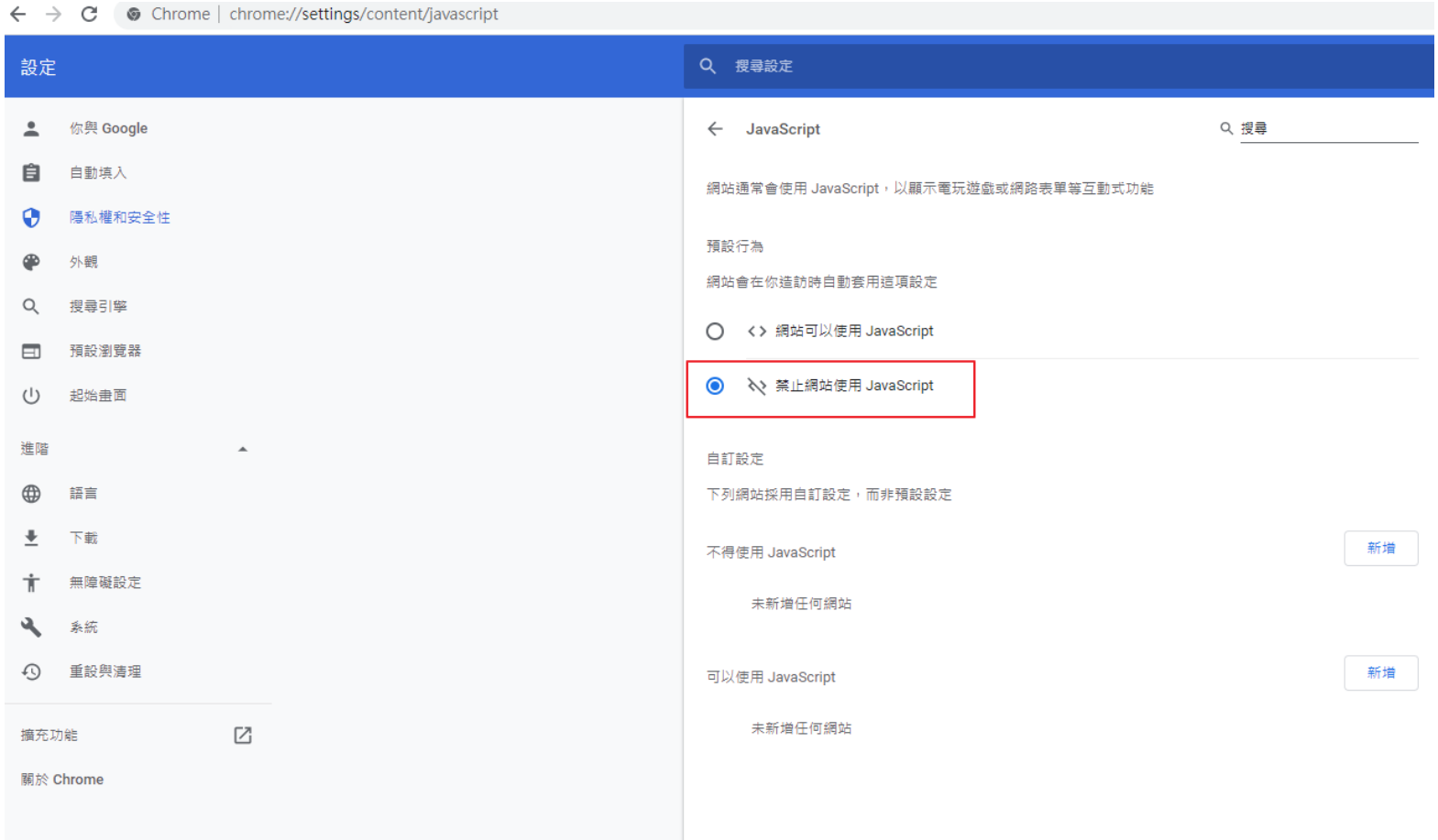
電腦安全管理建議

勒索軟體的散播途徑

勒索軟體目前主要的攻擊途徑:

- 惡意郵件
  - 釣魚連結和惡意夾檔
- 網頁掛馬
  - 遭駭客入侵的網站
  - 惡意廣告
- 弱點攻擊
  - Edge browser
  - Java /Flash
  - Adobe …

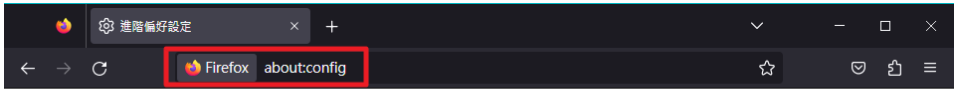
停用瀏覽器java、flash-Chrome



停用瀏覽器 java、flash－Firefox(1/2)

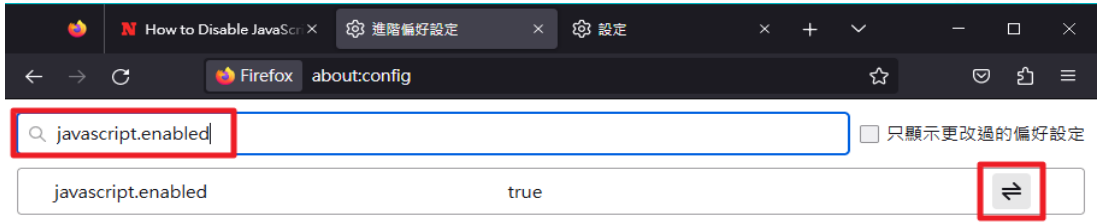
二、在 Firefox 中停用 Java、Flash：

第1步 開啟 Firefox 瀏覽器，搜尋「**about:config**」，並點選「**接受風險並繼續**」。



停用瀏覽器java、flash－Firefox(2/2)

第2步 搜尋「javascript.enabled」，並點選右邊按鈕，將此功能關閉。

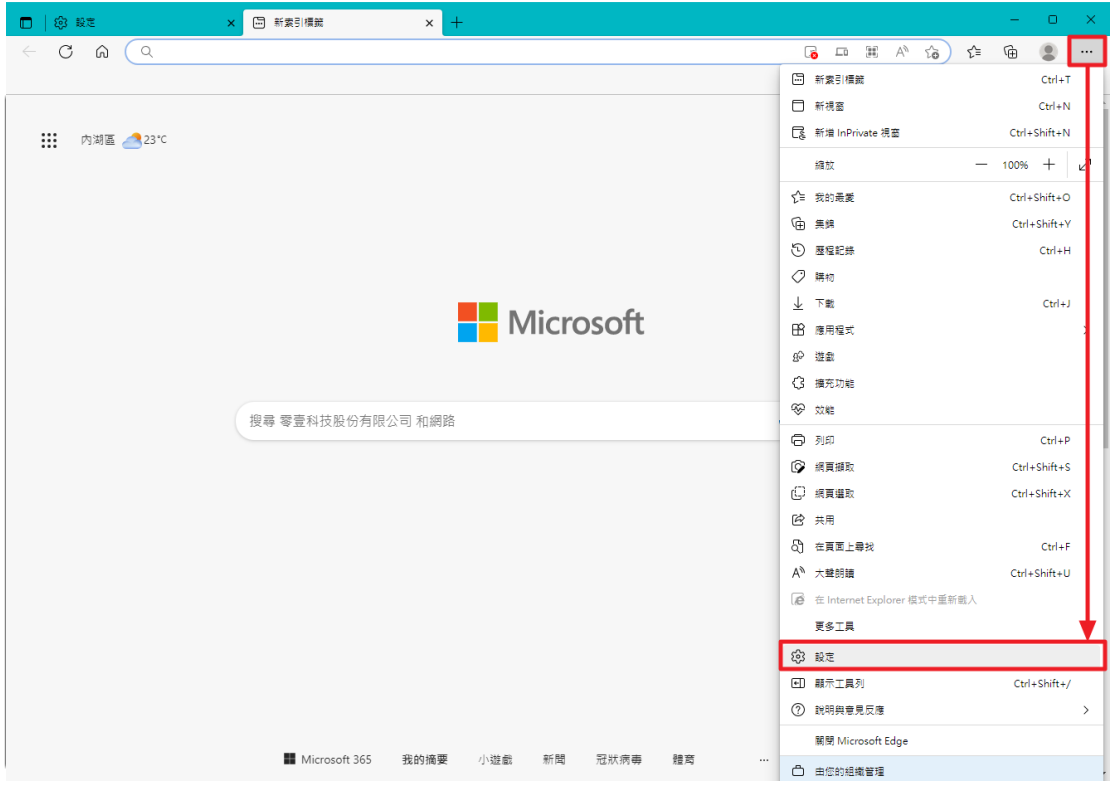


加強瀏覽器安全 - Firefox

停用瀏覽器 java、flash－Edge(1/2)

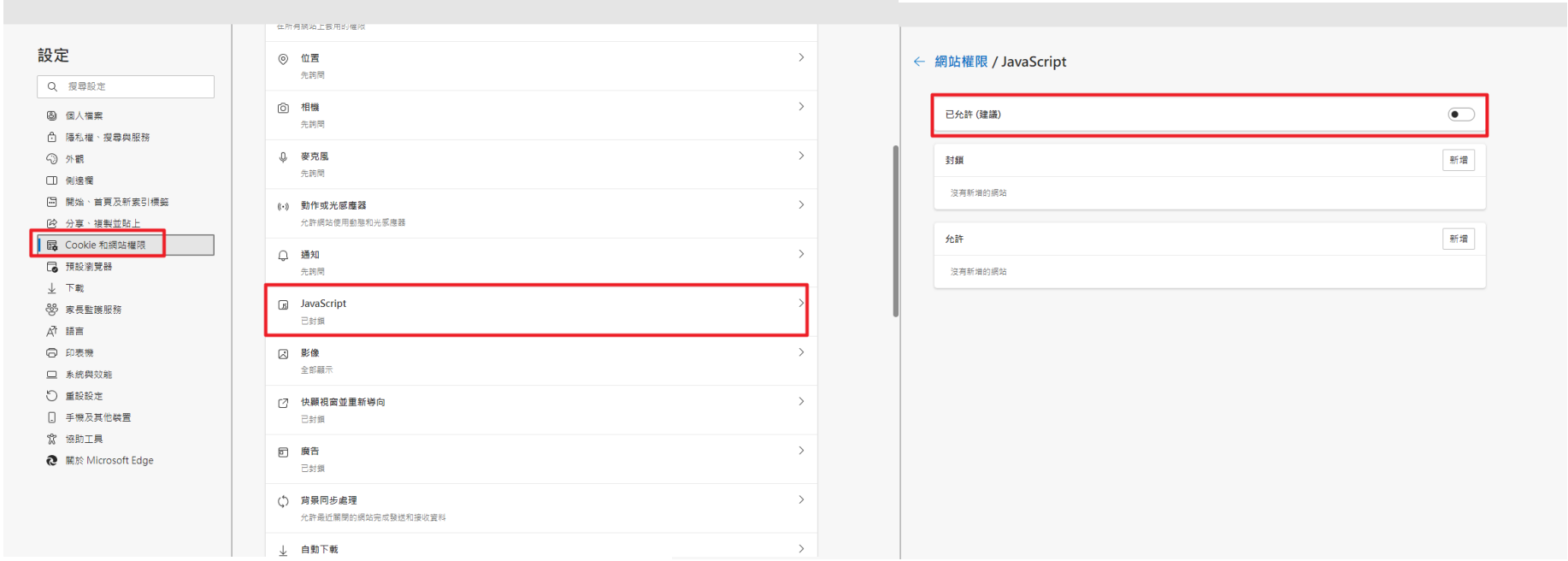
三、在 Edge 中停用 Java、Flash：

第1步 開啟 Microsoft Edge 瀏覽器視窗，點一下右上角「···」圖示，選擇「**設定**」。

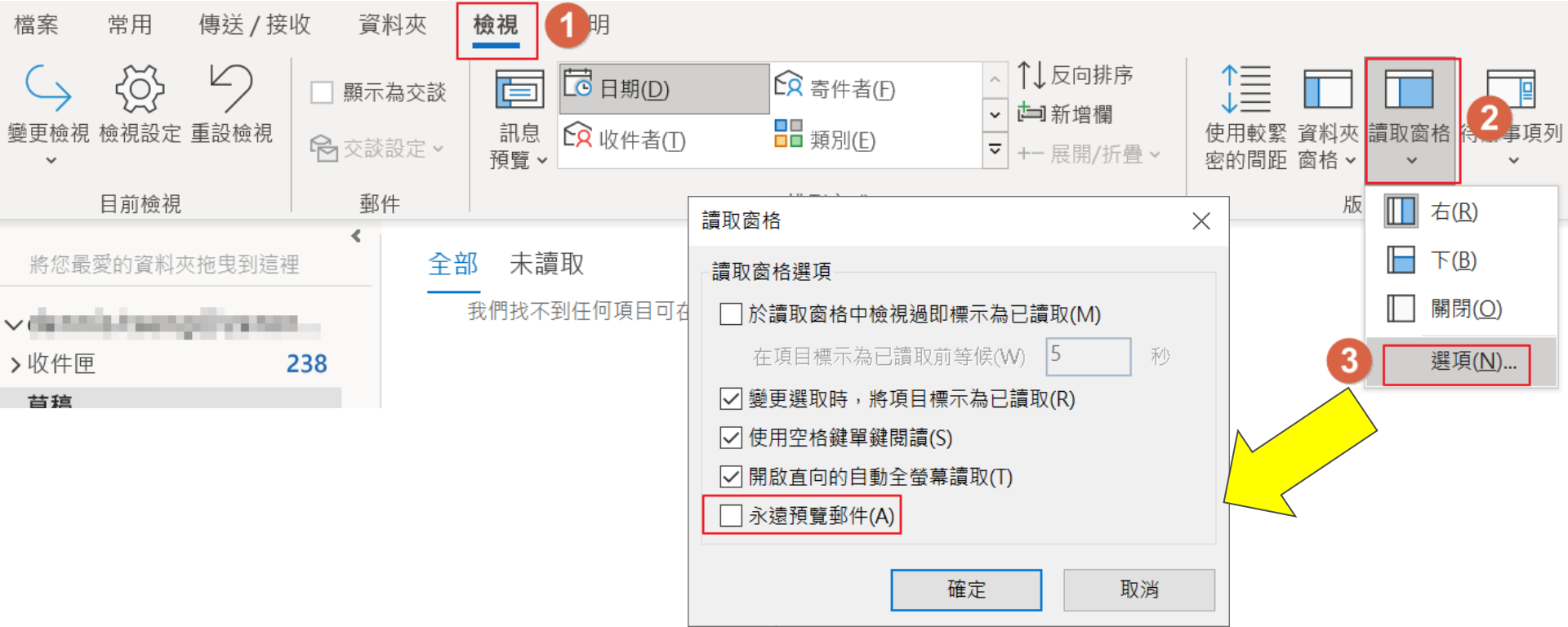


停用瀏覽器 java、flash - Edge(2/2)

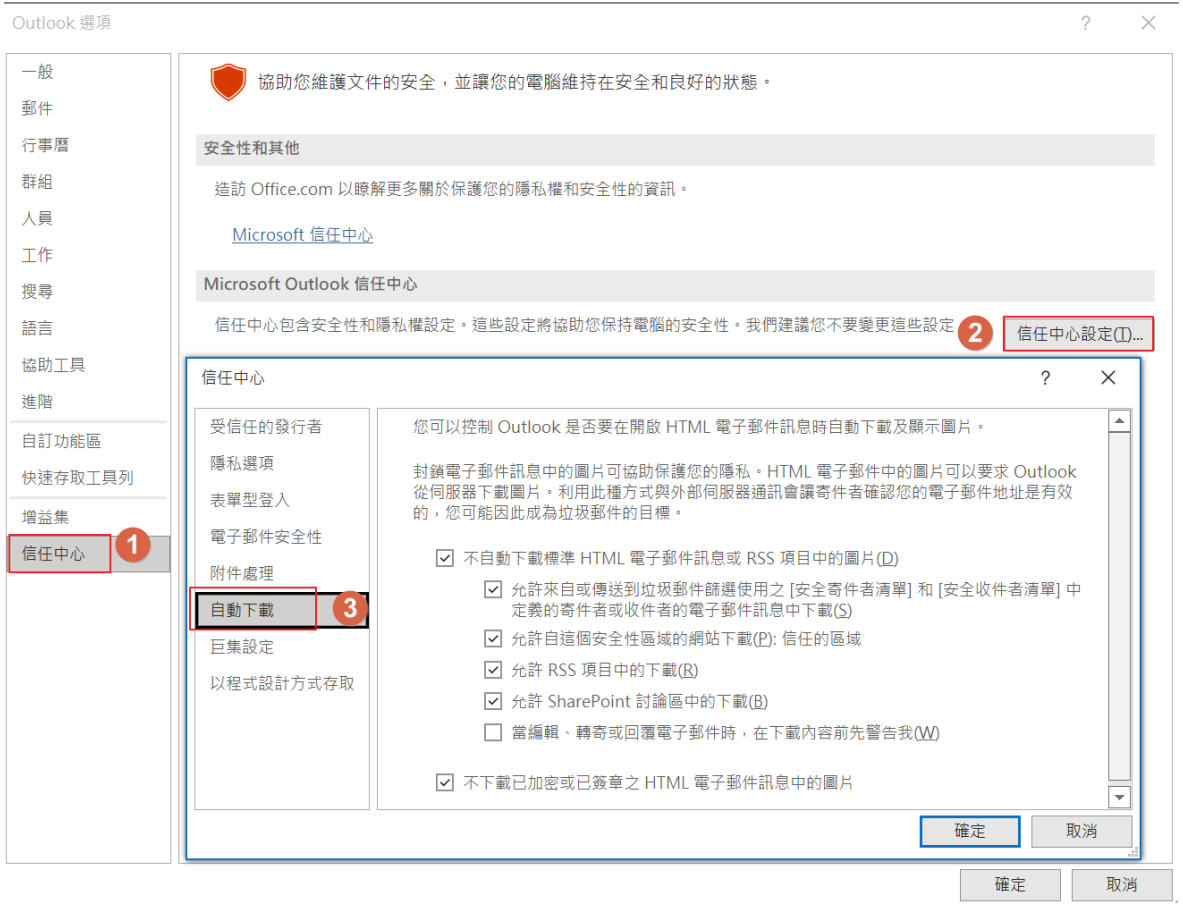
第2步 在「Cookie 和網站權限」選單中，找到並點擊要停用的項目，將它關閉。



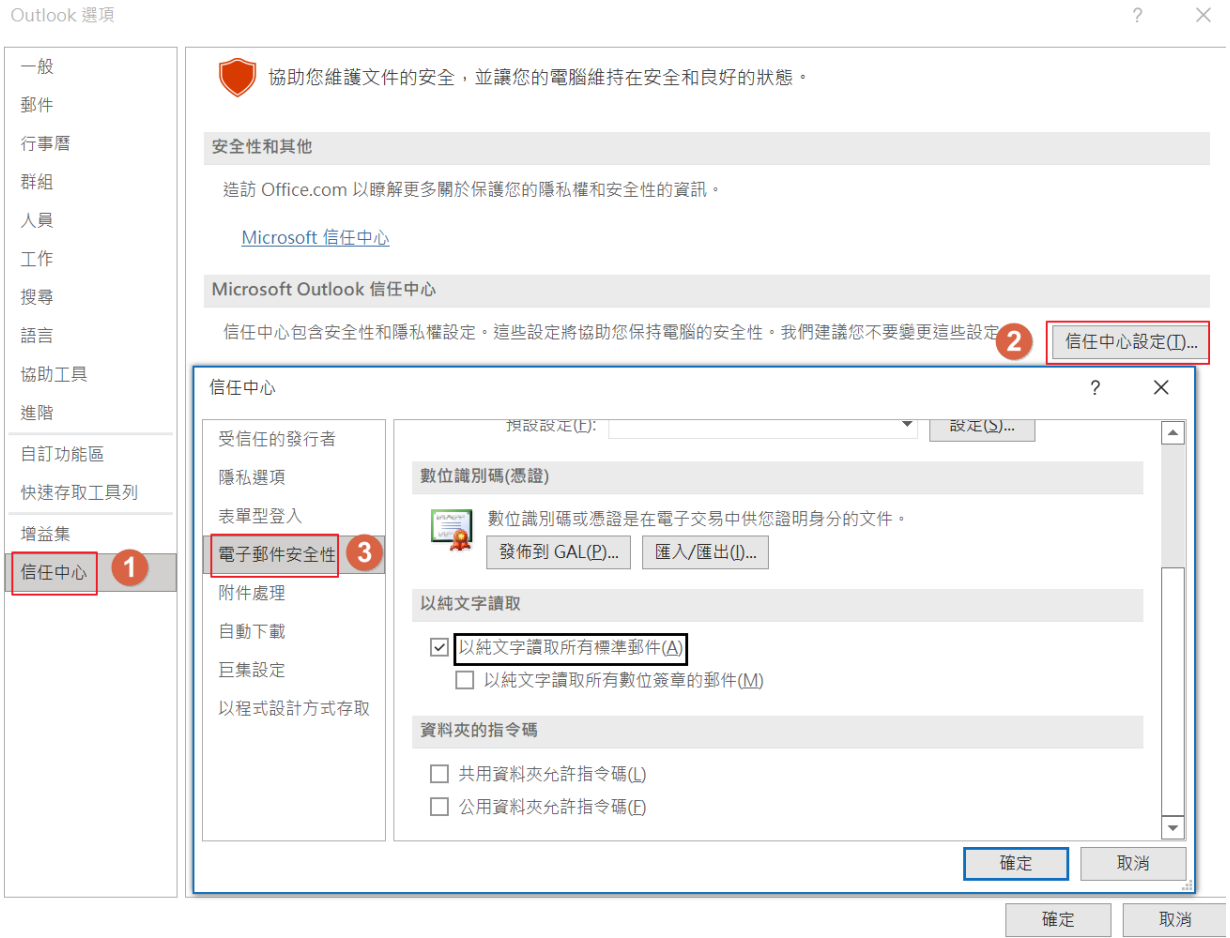
收信軟體安全-關閉預覽視窗(Outlook)



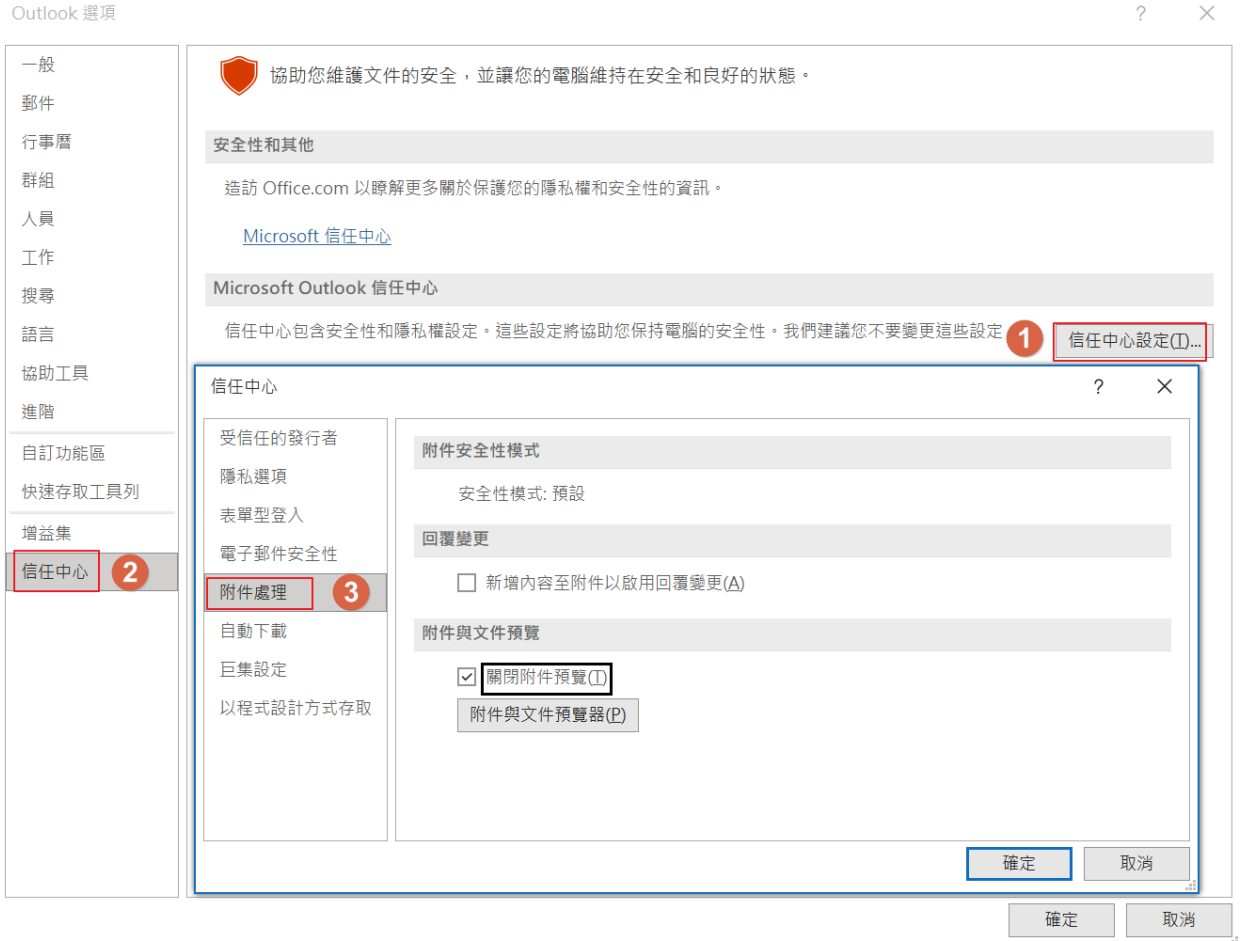
收信軟體安全-關閉自動圖片下載(Outlook)



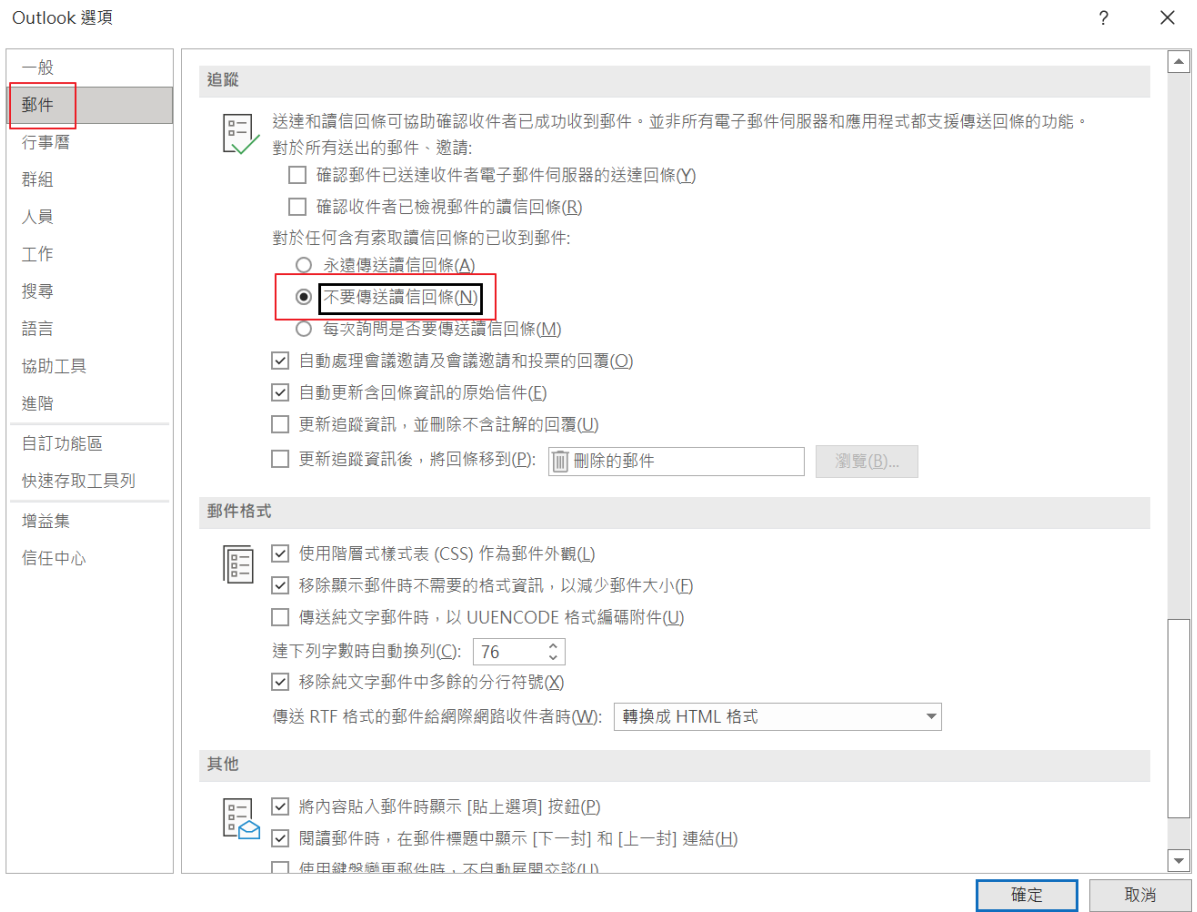
收信軟體安全-以純文字閱讀(Outlook)



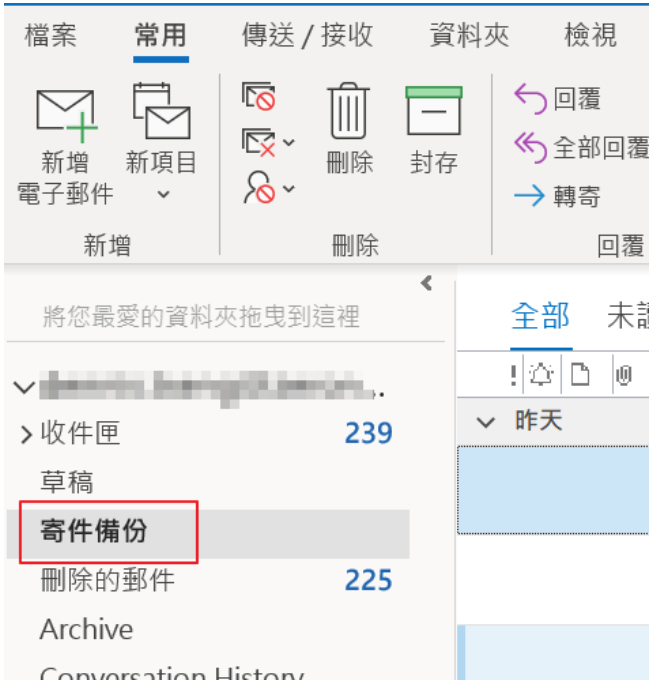
收信軟體安全-關閉附件預覽(Outlook)

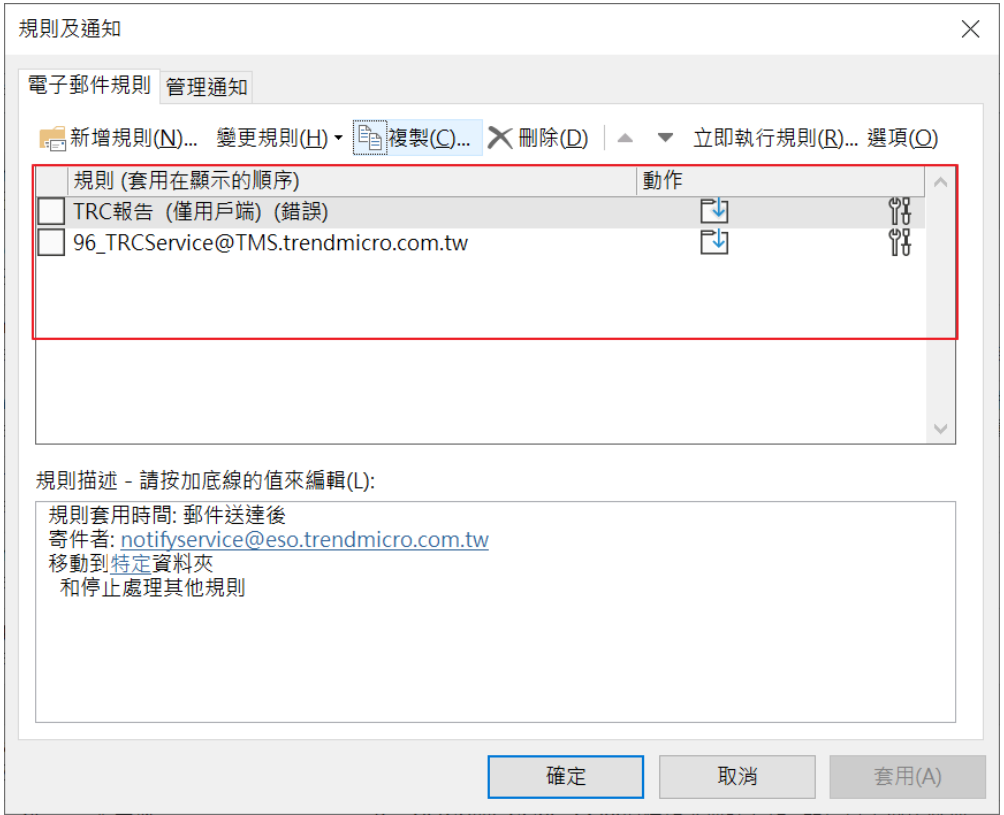


收信軟體安全-不要自動回覆讀信回條(Outlook)



收信軟體安全-不定時檢查寄件備份與郵件規則(Outlook)





休息一下

台灣網路資訊中心(TWNIC)資安新聞_2022.3.7
8個字元長度的複雜密碼僅需一小時即可破解

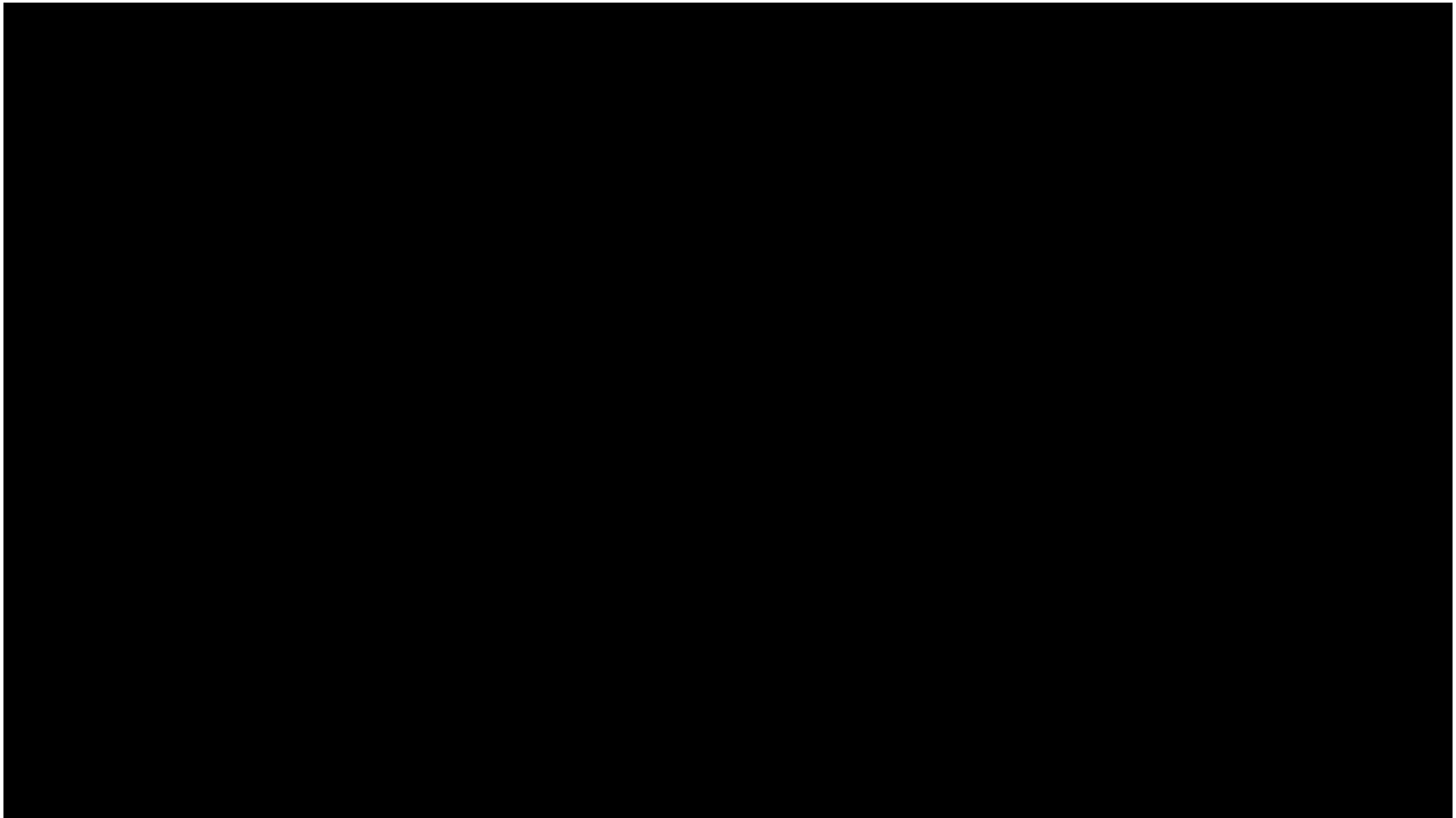
資安廠商指出，8 個字元長度的複雜密碼，最新繪圖卡僅需一小時即可破解

發布日期：2022-03-07 字型大小： 小 中 大

發布單位:TWCERT/CC 更新日期:2022-03-23 點閱次數:1049

資安廠商 **HIVE SYSTEMS** 日前發表研究報告指出，運用市場上最新的強大繪圖卡，來模擬進行密碼 **MD5** 比對，駭侵者將能在 **1** 小時內破解包含大小寫字母與數字的 **8** 位數字元密碼。

密碼安全



密碼的安全性

- 密碼設定難一點(符合長度與複雜度的條件)並定期更換密碼
- 更換的密碼不與先前的密碼重複
- 所謂複雜度就是一串密碼當中包了以下的字元種類

數字 0~9

英文小寫 a~z

英文大寫 A~Z

特殊字元 如：~!@#$%^&*()...此類字元

舉例：123QAZwsx!!@@##

密碼的其他建議

- **對應中文輸入法的密碼**

說明：先想定中文字以後依照鍵盤上的字根定義密碼

舉例：我愛你，對應注音輸入法後得到【ji394su3】

缺點：沒看鍵盤時可能會一時之間想不起密碼

- **邏輯性(推薦)**

說明：常用高強度密碼配合**服務名稱**

舉例：123QAZwsx!!@@##Google

進階例1：123QAZwsx!!@@##Go0gl1

進階例2：123QAZwsx!!@@##F@c1bo0k

密碼不安全行為

密碼不安全行為


デザイン案 作成
見積書
14:00～ ミーティング
Password：01234

ダメ


Password
Warningpoint2

Two-Factor Authentication (2FA)

雙重驗證可提供多一層保障，使罪犯較難進行未授權的存取動作

在 2FA 的管制下，單憑使用者帳密無法登入，

您還需要第二項「驗證因素」：

① 僅限您個人知道的資訊(例如母親的本姓)

② 您個人持有的事物 (如簡訊發送的認證碼)

③ 應用程式或軟體保護鎖 [dongle])

④ 或是駭客無法取得的個人特徵 (如指紋)

雙重驗證

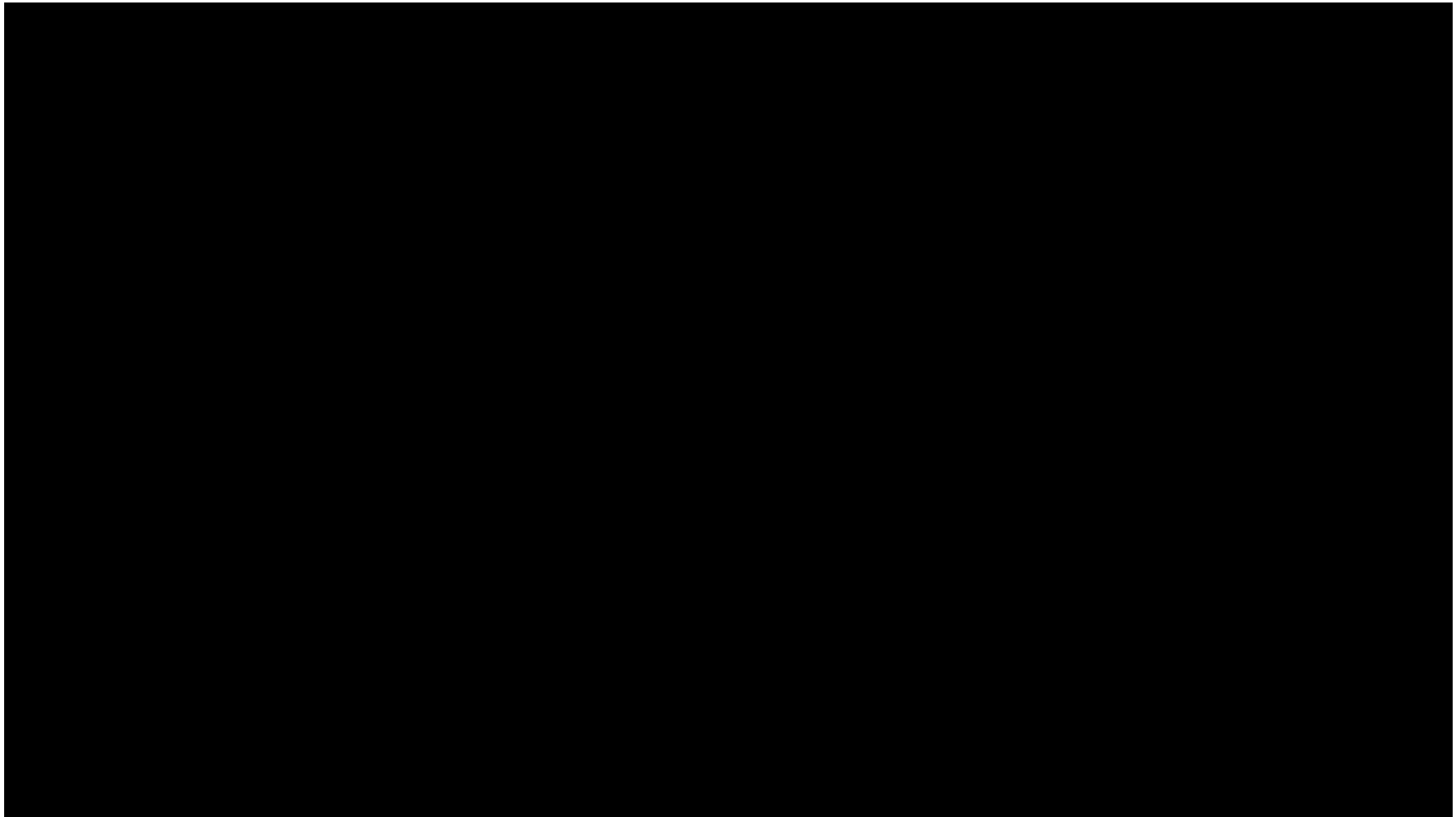
上網隱私

資料隱私一直以來都很重要。

我們現在花在網上的時間太多，在網上讓人瀏覽的個人資料也比以往任何時候都還要多。

因此了解資料隱私權並且採取必要措施來保護資料也就比以往都更為重要。

上網隱私



如何保護你的資料隱私權?

- 只將資料提供給可信任的公司或網站
- 分享前要三思
- 利用隱私設定
- 使用強密碼並啟用雙因子認證（2FA）
- 使用公共熱點時善用VPN

如何預防勒索軟體? 3-2-1

三要

- 要定期備份重要的檔案（321法則）
- 要定期更新修補作業系統與應用程式的漏洞
  Java/Flash/Adobe/Windows update
- 要安裝防毒啟用防勒索行為控管

兩不

- 不開放共享資料夾寫入權限
- 不共用帳號

一宣導

- 同仁社交工程警覺訓練, 尤其是網站及郵件的相關警覺及認知
- 只打開信任的郵件 不隨意打開未知來源信件的連結以及附件

被勒索當下緊急應變措施

- 斷網- 斷開網路連線
- 斷電- 馬上關機 （5分鐘內還有資料可以救回..看電腦速度）
- 保留電腦 通報資訊人員
- 斷Account ， 暫時停止該員電腦網路存取登入權限
- 檢查該員權限可以寫入公用資料夾是否感染
- 資料備份還原 /外接HD救資料
- 使用ATTK 掃描後送趨勢分析

勒索軟體-解密工具

Trend Micro Ransomware File Decryptor

Crypto Ransomware 是一種勒索程式，它可以加密檔案，令用戶不能使用有關檔案。要再次使用檔案，受害用戶會被要求交出贖款。趨勢的解密工具可解除部分的 Crypto Ransomware 的變種勒索程式，讓用戶不須交付贖款。

勒索軟體-解密工具

- 支援解密的勒索病毒家族

CryptXXX V1, V2, V3*	{original file name}.crypt, cryp1, crypz, or 5 hexadecimal characters
CryptXXX V4, V5	{MD5 Hash}.5 hexadecimal characters
TeslaCrypt V1	{original file name}.ECC
TeslaCrypt V2	{original file name}.VVV, CCC, ZZZ, AAA, ABC, XYZ
TeslaCrypt V3	{original file name}.XXX or TTT or MP3 or MICRO
TeslaCrypt V4	File name and extension are unchanged
SNSLocker	{Original file name}.RSNSLocked
AutoLocky	{Original file name}.locky
BadBlock	{Original file name}
777	{Original file name}.777
XORIST	{Original file name}.xorist or random extension

Nemucod	{Original file name}.crypted
Chimera	{Original file name}.crypt
LECHIFFRE	{Original file name}.LeChiffre
MirCop	Lock.{Original file name}
Jigsaw	{Original file name}.random extension
Globe/Purge	V1: {Original file name}.purge V2: {Original file name}.{email address + random characters} V3: Extension not fixed or file name encrypted
DXXD	V1: {Original file name}.{Original extension}dxxd
Teamxrat/Xpan	V2: {Original filename}.__xratteamLucked
Crysis	.{id}.{email address}.xtbl, .{id}.{email address}.crypt, .{id}.{email addres}.dharma, .{id}.{email address}.wallet
TeleCrypt	{Original file name}
DemoTool	.demoadc
WannaCry (WCRY)	{Original file name}.WNCRY, {Original file name}.WCRY
Petya	N/A

勒索軟體-解密工具

注意事項：

- 被 CryptXXX V3加密的檔案，可能無法完整還原成原始檔案(部分解密)。 詳細可參閱 [**關於 CryptXXX V3 重要說明**]
- RansomwareFileDecryptor 1.0.xxxx MUI僅能解密 TeslaCrypt V3、TeslaCrypt V4。
- 解密前備份；從單一檔案或資料夾開始解密

勒索軟體-解密工具

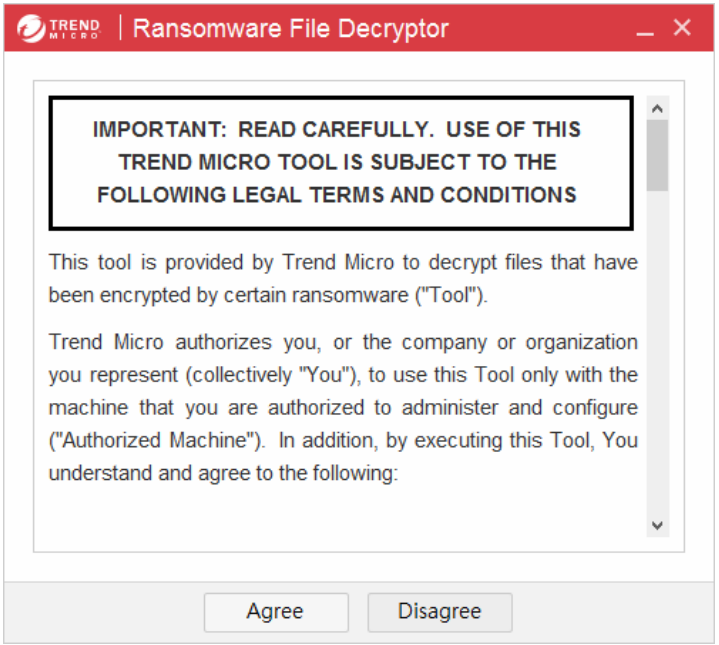
工具下載：

- 點選 **勒索病毒檔案解密工具(RansomwareFileDecryptor)** 取得最新版本趨勢科技勒索病毒檔案解密工具。
- 工具完整詳細說明

https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

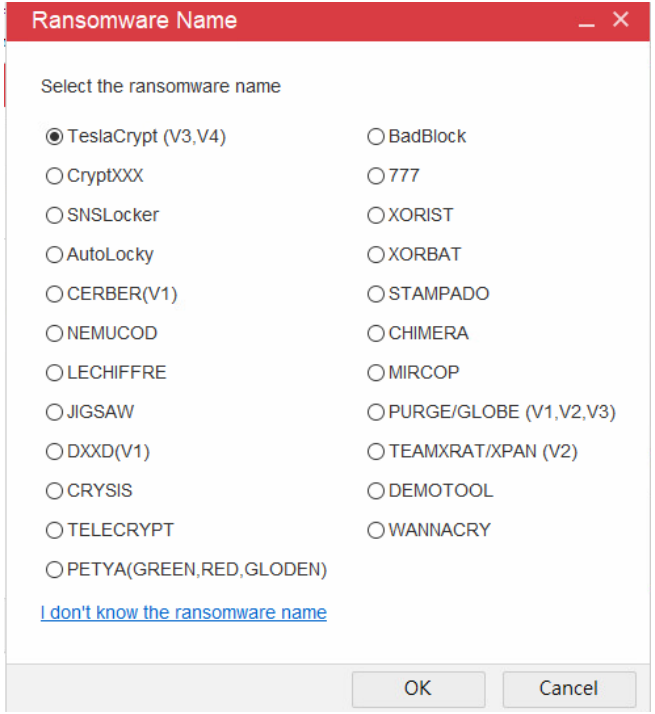
勒索軟體-解密工具

- 下載解密工具 RansomwareFileDecryptor 1.0.1668 MUI.zip
- 解壓縮後執行RansomwareFileDecryptor 1.0.1668 MUI.exe



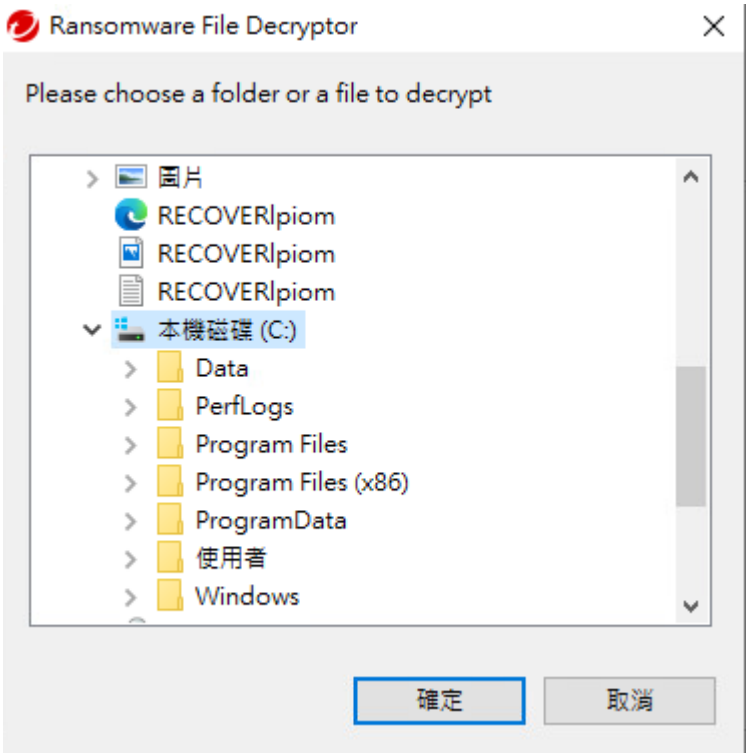
勒索軟體-解密工具

- 選擇解密類型



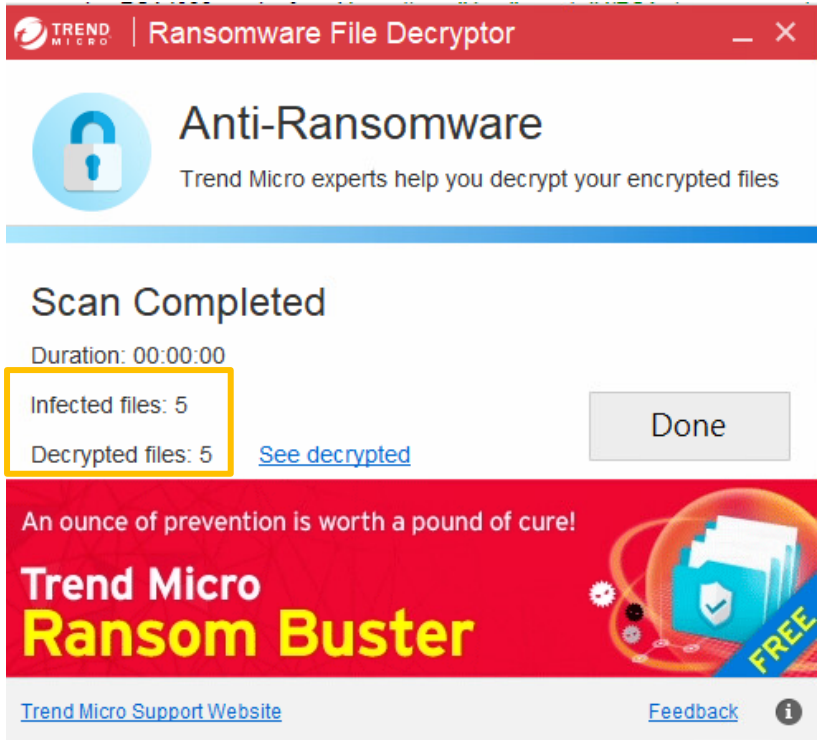
勒索軟體-解密工具

- 選擇要解密檔案或目錄



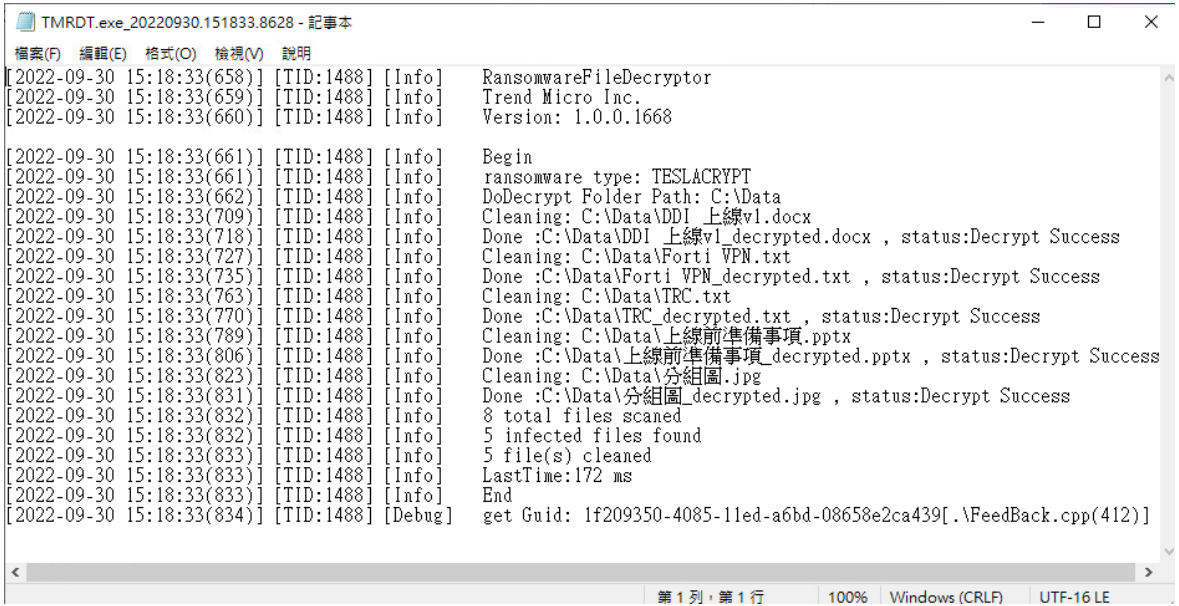
勒索軟體-解密工具

- 檔案解密，掃描完成。

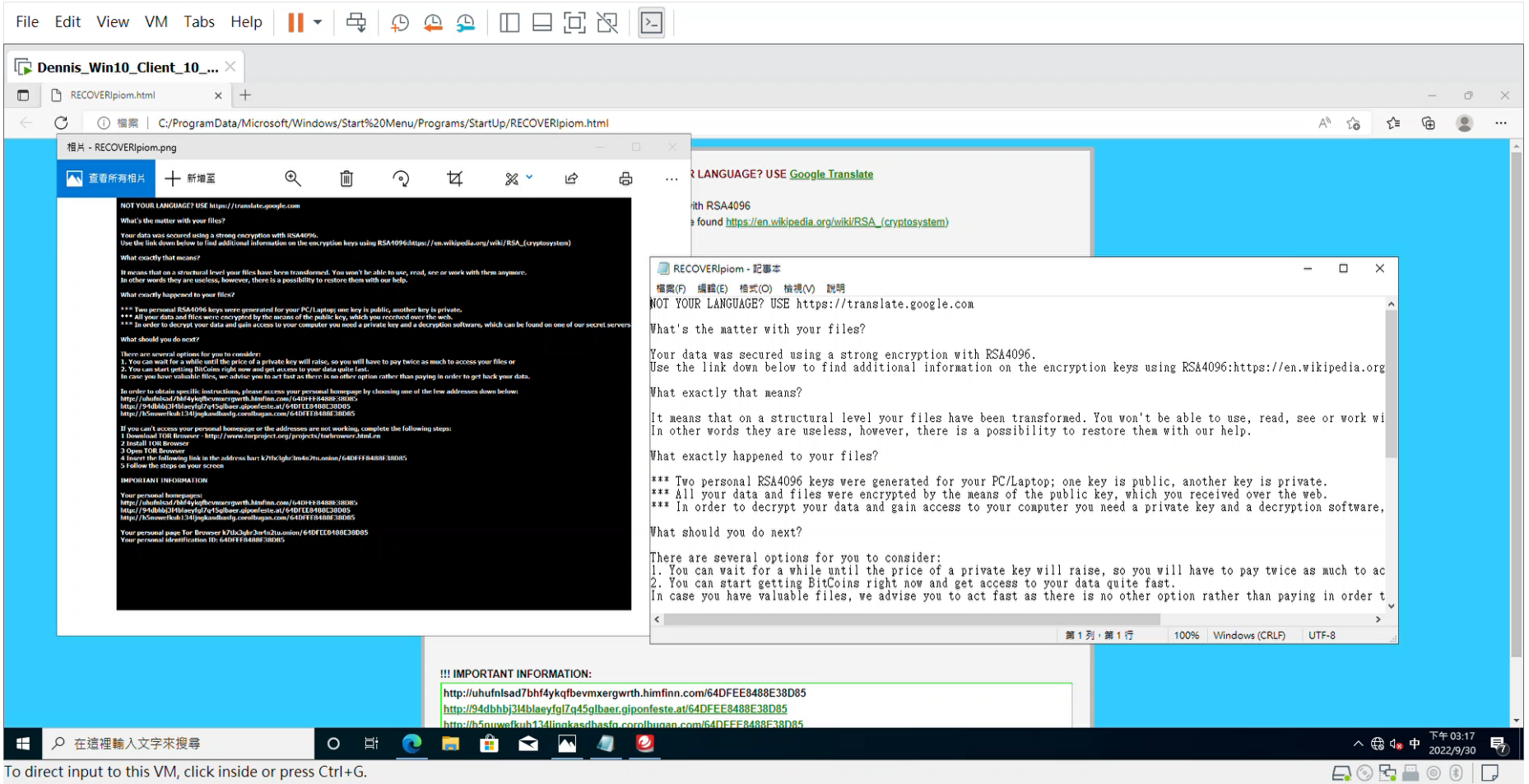


勒索軟體-解密工具

- 工具記錄檔
  %User%\AppData\Local\Temp\TMRDTSelfExtract\LOG



解密工具操作影片


File Edit View VM Tabs Help
Dennis_Win10_Client_10_...
RECOVERIpiom.html
C:/ProgramData/Microsoft/Windows/Start%20Menu/Programs/StartUp/RECOVERIpiom.html
相片 - RECOVERIpiom.png
查看所有相片
新增至
NOT YOUR LANGUAGE? USE https://translate.google.com
What's the matter with your files?
Your data was secured using a strong encryption with RSA4096.
Use the link down below to find additional information on the encryption keys using RSA4096:https://en.wikipedia.org/wiki/RSA_(cryptosystem)
What exactly that means?
It means that on a structural level your files have been transformed. You won't be able to use, read, see or work with them anymore.
In other words they are useless, however, there is a possibility to restore them with our help.
What exactly happened to your files?
*** Two personal RSA4096 keys were generated for your PC/Laptop one key is public, another key is private.
*** All your data and files were encrypted by the means of the public key, which you received over the web.
*** In order to decrypt your data and gain access to your computer you need a private key and a decryption software, which can be found on one of our secret servers
What should you do next?
There are several options for you to consider:
1. You can wait for a while until the price of a private key will raise, so you will have to pay twice as much to access your files or
2. You can start getting BitCoins right now and get access to your data quite fast.
In case you have valuable files, we advise you to act fast as there is no other option rather than paying in order to get back your data.
In order to obtain specific instructions, please access your personal homepage by choosing one of the few addresses down below:
http://uhufnlsad7bhf4ykqfbevmxergwrth.himfinn.com/64DFEE8488E38D85
http://94dbhbj3l4blaeyfgl7q45glbaer.giponfeste.at/64DFEE8488E38D85
http://h5nuwefkuh134ljngkasdbasfg.corolbugan.com/64DFEE8488E38D85
If you can't access your personal homepage or the addresses are not working, complete the following steps:
1 Download TOR Browser - http://www.torproject.org/projects/torbrowser.html.en
2 Install TOR Browser
3 Open TOR Browser
4 Insert the following link in the address bar: k7ibx3ghr3m4n2tu.onion/64DFFE8488E38D85
5 Follow the steps on your screen
IMPORTANT INFORMATION
Your personal homepages:
http://uhufnlsad7bhf4ykqfbevmxergwrth.himfinn.com/64DFEE8488E38D85
http://94dbhbj3l4blaeyfgl7q45glbaer.giponfeste.at/64DFEE8488E38D85
http://h5nuwefkuh134ljngkasdbasfg.corolbugan.com/64DFEE8488E38D85
Your personal page Tor Browser k7ibx3ghr3m4n2tu.onion/64DFEE8488E38D85
Your personal identification ID: 64DFFE8488E38D85
R LANGUAGE? USE Google Translate
ith RSA4096
e found https://en.wikipedia.org/wiki/RSA_(cryptosystem)
RECOVERIpiom - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
NOT YOUR LANGUAGE? USE https://translate.google.com
What's the matter with your files?
Your data was secured using a strong encryption with RSA4096.
Use the link down below to find additional information on the encryption keys using RSA4096:https://en.wikipedia.org
What exactly that means?
It means that on a structural level your files have been transformed. You won't be able to use, read, see or work wi
In other words they are useless, however, there is a possibility to restore them with our help.
What exactly happened to your files?
*** Two personal RSA4096 keys were generated for your PC/Laptop; one key is public, another key is private.
*** All your data and files were encrypted by the means of the public key, which you received over the web.
*** In order to decrypt your data and gain access to your computer you need a private key and a decryption software,
What should you do next?
There are several options for you to consider:
1. You can wait for a while until the price of a private key will raise, so you will have to pay twice as much to ac
2. You can start getting BitCoins right now and get access to your data quite fast.
In case you have valuable files, we advise you to act fast as there is no other option rather than paying in order t
第 1 列，第 1 行
100%
Windows (CRLF)
UTF-8
!!! IMPORTANT INFORMATION:
http://uhufnlsad7bhf4ykqfbevmxergwrth.himfinn.com/64DFEE8488E38D85
http://94dbhbj3l4blaeyfgl7q45glbaer.giponfeste.at/64DFEE8488E38D85
在這裡輸入文字來搜尋
下午 03:17
2022/9/30
To direct input to this VM, click inside or press Ctrl+G.

簡單、直覺的登入帳號方式，背後的潛在威脅

使用雲端帳號登入應用程式的三大風險

- 臉書中透露大量的個人資訊，包括姓名、身份、關係狀態、工作經歷、動態時報貼文皆是公開的，第三方應用程式可以從中蒐集使用者的完整資料。
- 沒辦法確保第三方應用程式取得哪些資訊，並且作為何種用途。
- 使用同一個臉書帳號登入，一旦被駭客入侵所有個資皆會同時被竊取。

駭客如何利用員工的社群網站入侵公司

公用電腦

- 使用與他人共用的電腦時，記得登出 Facebook。
- 不小心忘了登出，可以使用遠端登出功能。

移除Facebook 與應用程式間的連結

安全性設定

Google 帳戶

在 Google 帳戶中搜尋

- 首頁
- 個人資訊
- 資料和隱私權
- 安全性
- 使用者和分享內容
- 付款和訂閱
- 關於

安全性

協助您確保帳戶安全的設定和建議

您有可參考的資安建議

安全設定檢查工具已偵測到問題，建議您採取必要的行動

保護您的帳戶

近期的安全性活動

過去 28 天內沒有任何安全性活動或警示

安全性設定

登入 Google

密碼	上次變更時間：6月8日
兩步驟驗證	已開啟
應用程式密碼	1 組密碼

我們可用來驗證您身分的方式

我們會透過這些方法確認登入帳戶的是您本人，或是在帳戶出現可疑活動時與您聯絡

備援電話號碼	09 5
備援電子郵件	請驗證 k @gmail.com

安全性設定

您的裝置

已登入帳戶的裝置

在 Windows 電腦上有 1 個工作階段
Windows

在 Android 手機上有 1 個工作階段
As[redacted]lax
M[redacted]

尋找遺失的裝置

管理所有裝置

具有帳戶存取權的第三方應用程式

您已授權下列網站和應用程式存取您的部分 Google 帳戶資料 (可能包括機密資訊)。如果當中有您不再信任或使用的網站或應用程式，請移除這些項目的存取權。

diagrams.net (draw.io)
可以存取下列服務：Google Drive

管理第三方存取權

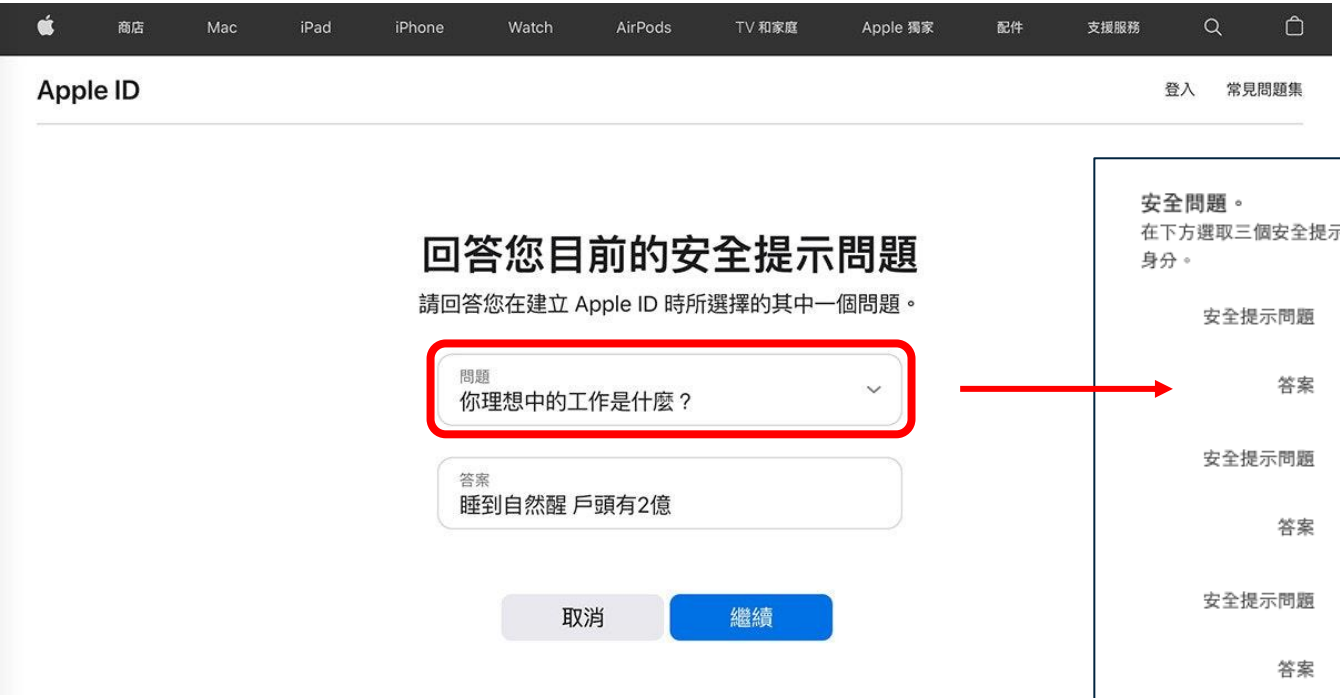
為您的帳戶啟用安全瀏覽強化防護功能

提供更貼近個人需求的保護機制，協助防範危險的網站、下載內容和擴充功能。

已關閉

管理安全瀏覽強化防護功能

安全提示問題


商店
Mac
iPad
iPhone
Watch
AirPods
TV 和家庭
Apple 獨家
配件
支援服務
Apple ID
登入
常見問題集
回答您目前的安全提示問題
請回答您在建立 Apple ID 時所選擇的其中一個問題。
問題
你理想中的工作是什麼？
答案
睡到自然醒 戶頭有2億
取消
繼續


安全問題。
在下方選取三個安全提示問題。當您忘記密碼時，這些安全提示問題可幫助我們確認您的身分。
安全提示問題
你少年時期最好的朋友叫什麼名字？
答案
****
安全提示問題
你擁有的第一台車是什麼型號？
答案
****
安全提示問題
你的父母親是在哪個城市認識的？
答案
****

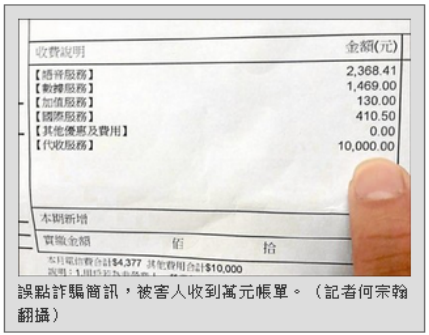
行動裝置安全與上網安全

新聞事件

不識詐騙簡訊 連點10次一萬飛了

2014-06-23

〔記者姚岳宏、何宗翰／綜合報導〕電信詐騙推陳出新，新一波的詐騙簡訊App要求使用者「下載」程式才能查看照相或罰單紀錄；也有歹徒冒名警察局發簡訊詐騙，有人點擊連結沒有反應，連點了10次，收到帳單才發現被騙了1萬元。



誤點詐騙簡訊，被害人收到萬元帳單。（記者何宗翰翻攝）

刑事局指出，近期出現以手機簡訊、LINE及WeChat（微信）發送「您的汽機車有交通罰單未繳，查一查自己有無莫名被照相或罰款的紀錄」，有民眾一時好奇，依指示下載App，等隔月收到帳單無故多了「小額付款交易」，才知是詐騙伎倆。

新竹市警局中華派出所本月接獲10起網路詐騙案，全都是以「新北市警察局」名義，發簡訊詐騙，有人還因點擊10次，被騙1萬元。

刑事局呼籲，不管這些惡意程式包著什麼糖衣，不要點選任何連結，才是自保的不二法

作騙手法鎖定車主　交通罰單簡訊恐遭騙


放大照片

詐騙簡訊猖獗，現在又有新的詐騙手法，這次鎖定有車一族。新北市交通事件裁決處發現，最近來電詢問是否有罰單逾期未繳的民眾明顯增多，共通點就是車主紛紛收到查詢罰款紀錄的簡訊，若不留心點選連結恐使個資遭竊。

「您好，您的汽機車有交通罰單逾期未繳納，查一查自己有無莫名其妙被照相或罰款的記錄，查詢下載http://g--.gl/VamU-

如果接到類似簡訊，得當心是詐騙集團找上門。

市交通事件裁決處表示，打電話到裁決處詢問詐騙簡訊的民眾明顯增加，因此特別提醒車公部門不會發送催繳交通罰單簡訊，應屬詐騙簡訊，研判目可能要竊取民眾的個資。

若須查詢是否有交通違規紅單時，可主動利用裁決處網站查詢，對被舉發事實有疑義時，可在網頁線上辦理申訴，填寫車號、違規單號、聯絡地址及陳述理由等相關資料，完成申訴程司時還可查詢申訴案件的處理進度。

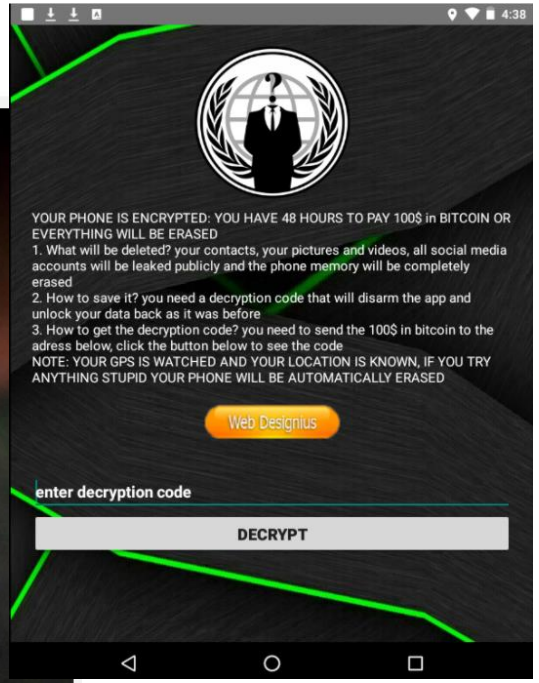
除了簡訊詐騙要當心，對於電話詐騙也不能掉以輕心，像是台北市一位74歲郭姓老婦人，接獲電話表示身分遭盜用，若要排除嫌疑必須提領戶頭內所有現金交付檢察官保管，以利案件偵辦，甚

新聞事件

勒索病毒現身大賺「疫情財」！不讓手機解鎖還會公開私密照

2020/03/17 07:39

文 / 記者黃肇祥



新聞事件

“48小時內支付贖金，否則你手機上的所有資料將永久被破壞！”又一手機勒索軟體現身

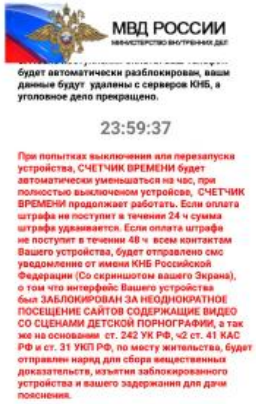
發表於 2014 年 06 月 25 日 由 Trend Labs 趨勢科技全球技術支援與研發中心

Android勒索軟體利用Tor隱藏C&C通訊

不久前我們介紹過不給錢就讓手機變磚塊!勒索集團威脅瀏覽色情網站 Android手機用戶，最近出現在行動威脅環境的勒索軟體現在有了新發展：利用TOR（The Onion Router）匿名服務來隱藏C&C通訊。

網上的連結別亂點！微軟曝新型Android勒索病毒 誤點恐讓手機Home鍵、螢幕癱瘓

王 佐銘
2020年10月14日 · 1分鐘 (閱讀時間)



匯流新聞網記者王佐銘 / 綜合報導

行動裝置中主要的勒索病毒類型

Lock Screen

File Encryption

PIN Hijack

針對行動裝置的勒索病毒感染來源

- 第三方應用程式商店
  - 最常見的途徑是透過第三方應用商店下載到勒索病毒
  - 官方的 Google Paly、Apple App Store 中尚未發現已被感染的App
- 社群網路
  - 傳遞的訊息中夾帶了惡意連結，使用者在不知覺的情況下開啟連結下載勒索病毒

詐騙簡訊類型

- 「嚇唬你讓你想確認」

  【新北市政府警察局通知單】您涉嫌的案件處理結果通知單。

  「尊敬的客戶您好，您的手機正在申請6800元的網絡支付，如非本人操作請加載電子憑證確認取消…」 。

  你的民事賠償訴訟通知單【台北地院】

- 「免費貼圖、人氣投票或按讚」

  “fb 免費送貼圖,把此消息轉發十五個 LINE 好友,可以免費領取價值一百的貼圖表情,加油吧,領取地址…”

  「○○○朋友家狗狗參加人氣比拼，幫忙讚一下」

  「學運受傷學生急需醫藥費！」

  「我的手機送修，麻煩替我收個簡訊好嗎？」

  「拜託收幾封購物簡訊，我有急用！」

詐騙簡訊類型


4G
完成
網飛
網飛
訊息
語音
視訊
郵件
其他
sg185splq67f3@mailer.mailingboss...
加入 VIP
封鎖此聯絡人
分享聯絡人
新增聯絡人
加入現有的聯絡人
分享我的位置


It's a FAKE!


POST
你好，
您的包裹無法在 2022 年 17 月 08 日寄出，因為尚未支付關稅（52.76 新台幣）
交貨時間安排在：21.06.2022 - 22.06.2022
金額：52.76 新台幣
收款人：中華郵政
要確認您的包裹已送達，請 單擊此處
如30日內未收到包裹，中華郵政有權要求每訂一天扣款（52.76新台幣）！
如需更多服務，請 單擊此處查找您的運輸跟踪
此電子郵件是自動發送的。 因此，不可能對他們做出回應。
謝謝你的信任，
您的中華郵政客服

詐騙簡訊類型


78% 11:43
0911517526
短訊息/多媒體訊息
2018年3月23日 星期五
您的花旗信用卡電子帳單傳遞失敗,請至網路銀行www.citibank.com.tw變更電子信箱.若連續六個月傳遞失敗,自次月起將改寄紙本帳單.
13:09

Line免費貼圖詐騙


FB免費送貼圖 把此消息轉發15個Line好友


waroo
Smile Brush 2
贈送
詐騙


facebook
電子郵件或電話
密碼
登录
建立新帳號
忘記密碼？
中文(简体) · 中文(台灣) · English (US) · 更多...
2013

假冒信件


待通知：國立中山大學正在與您共享文件
第 2 封郵件，共有 141 封
寄件者 國立中山大學
假冒中山大學名義發信
日期 今日 15:16
注意力，
您的文檔已在隊列中。
下載並登錄以發布您的文檔。
誘使您打開附檔
Zimbra Web Client Sign In nsy...
打開附檔出現登入網頁
zimbra
A SYNACOR PRODUCT
意圖騙取您的帳號密碼
Username:
Password:
Stay signed in
Sign In
Version:
Default
What's This? What's This?

假冒信件

MyCard安全性通知 收件匣 ×

MyCard <service@mycard520.com.tw>
寄給 我

MyCard安全性通知

**** 此信件由系統自動發送，請勿直接回覆****

親愛的會員您好：

您的會員帳號： c[redacted]@gmail.com

於 2018/4/15 上午 01:07:44 已成功登入會員。

如果這是您本人進行的登入，請忽略這個電子郵件。如果這不是您本人，為了確保您的帳戶安全，請您儘快登入會員更改密碼。

提醒您，MyCard會員帳號安全三步驟，建議您「不定期變更登入密碼、申請mySafe安全認證、確保綁定行動帳號」，謝謝。

立即登入MyCard會員，如有疑問，請您向MyCard客服人員反應，謝謝您。

MyCard 敬啟

LINE客服
ID
@mycard885
服務時間
24hr

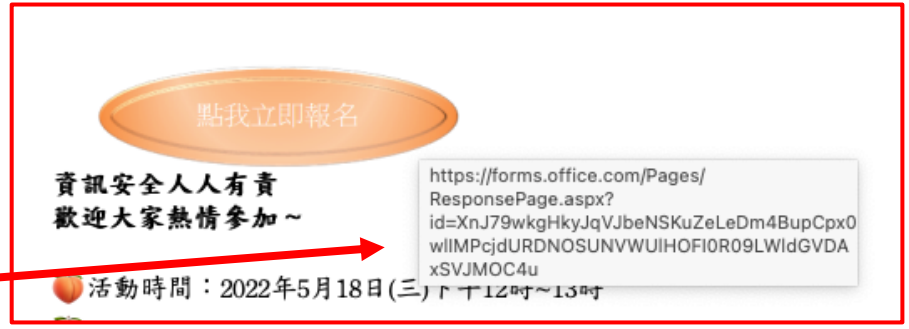
WeChat客服
ID
mycardcs
服務時間
24hr

MyCard 網站首頁 | MyCard 客服中心

假冒信件


2022年資安講座PART 1，請大家踴躍參加(送禮券) - 收件匣
刪除 封存 移動 標幟 標示為未讀取 同步處理
2022年資安講座PART 1，請大家踴躍參加(送禮券)
@zerone.com.tw>
收件者： 零壹科技全體同仁； 羽昇國際； 翊宇科技
Dears,
資安宣導講座又來囉!讓我們大家一起來提升資安素養，只要聽完整個課程即送禮卷 ~
此次邀請最有個人魅力的Podcast資安專家DJ Lin-林大鈞來跟大家分享，
聚焦資安主題，日常作業與資安風險的拉鋸，您不可不知的網路攻擊資安趨勢與案例、社交工程攻擊如何避免受騙、中毒…等
點我立即報名
資訊安全人人有責
歡迎大家熱情參加~
活動時間：2022年5月18日(三)下午12時~13時
只要符合以下條件，人人有獎
精美獎項：7-11禮券100元，符合參加標準，人人有獎，禮卷將於會後一個禮拜通知領取
參加方式：在任何有網路(非公司網路也可以)的情況下，不限裝置裝都可連線參加
得獎步驟 (以下將由科技數據做為判斷，不符標準，恕不贈送)
1 完整觀賞整個講座
2 會
當天直播連結底家，請於會議前2分鐘點我連線
Best Regards,
ZERONE 零壹科技
ZERO ONE TECH. CO., LTD

檢查連結


點我立即報名
資訊安全人人有責
歡迎大家熱情參加~
https://forms.office.com/Pages/ResponsePage.aspx?id=XnJ79wkgHkyJqVJbeNSKuZeLeDm4BupCpx0wlIMPcjdURDNOSUNVWUlHOFI0R09LWldGVDAxSVJMOC4u
活動時間：2022年5月18日(三)下午12時~13時


得獎步驟 (以下將由科技數據做為判斷，不符標準，恕不贈送)
1 完整觀賞整個講座
2
當天直播連結底家，請於會議前2分鐘點我連線
https://z1meeting.webex.com/z1meeting/j.php?MTID=m17a08c915b5a3682d37869b2ee6f9c37
Best Regards,

假冒網站


://facebook.co
hacker.com


如何分辨真假雄獅Facebook官方粉絲團
雄獅旅遊官方粉絲團
假粉絲團
雄獅旅遊Lion Travel
@lioncyber
已驗證粉絲專頁
Facebook 已確認此為這個企業或組織的真實粉絲專頁。
LION GROUP
雄獅旅遊
雄獅旅遊Taiwan
假粉絲團無Facebook官方驗證的灰勾勾

假冒網站


假網站
A
storeline4.weebly.com
LINE
LINE MOBILE


正版
B
tw.linemobile.com
LINE
LINE MOBILE
簡單辦 輕鬆賺
4G終身吃到飽
只要299起

假冒網站


官方正確網址應爲.gov.tw
https://www.mohw.gov.tw/
www.mohw.gov.tw
真
點擊網址前請注意網址
政府機關網址爲「.gov.t
釣魚連結/不明網頁
https://wsflbfqygov.xyz/?5m6c
twffgov.com
twbgov.com/hmex
https://sigov.top
https://cryptonvese.com
假
官方網址不會在「gov」前冠上
其他英文或數字，切勿點擊
不明連結網址及輸入個資
2022/08/31
衛生福利部
中央流行疫情指揮中心


94
outlook.com
【衛生局】您的補貼已通過
點 https://
www.trrgov.com 注冊提領
(複製網址到瀏覽器打開

假冒網站

為慶賀好市多#創造840億年營收

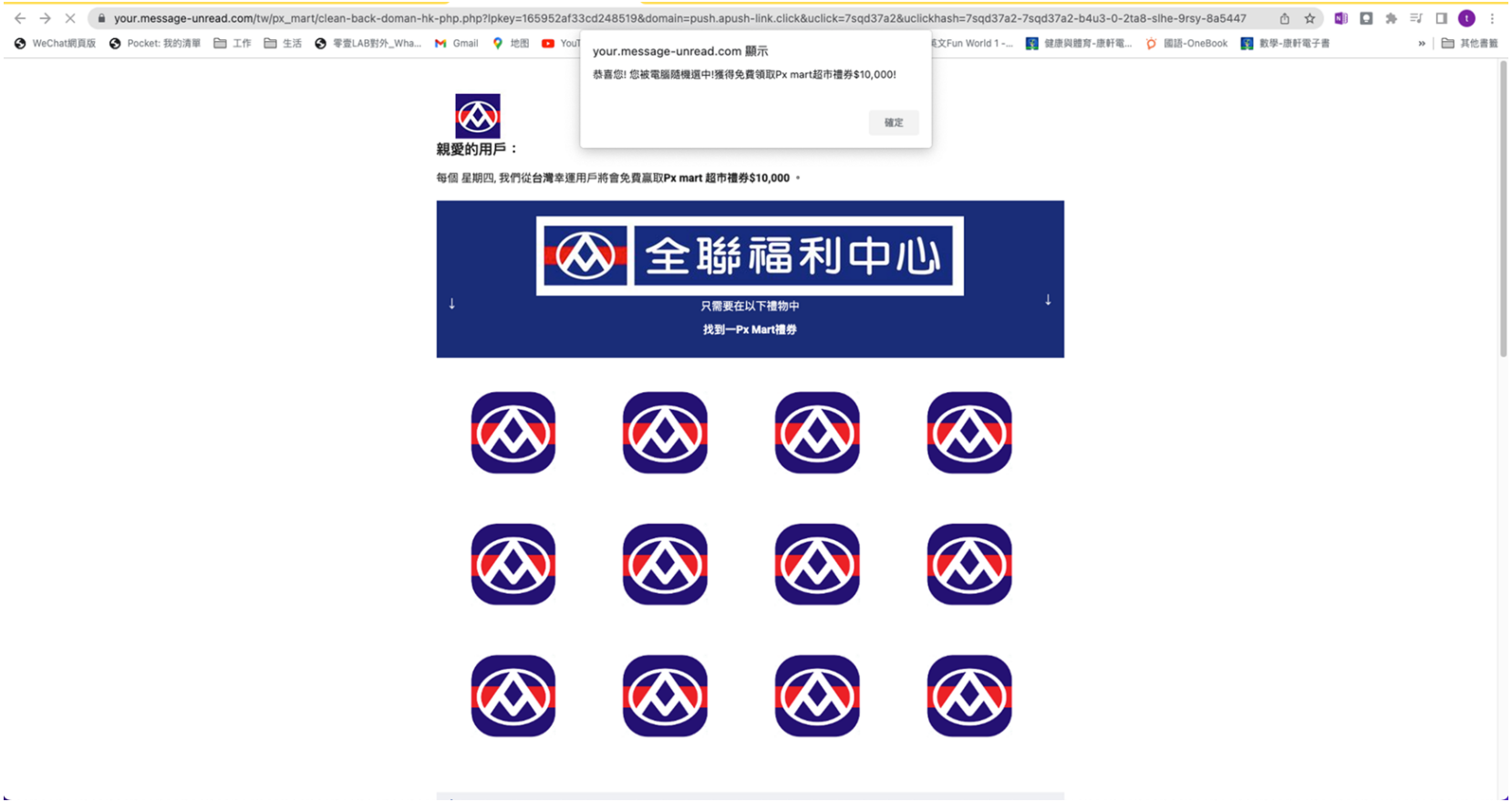
總裁決定每日推出20個AirPods3代"聯手"AirPods Pro雙拳出擊!

每人限購一次!

>>>>>>hxxps://vip(.)mascotnow(.)online/twcostco

【贈送虎年保護殼】新年特惠每人限購一次!

假冒網站


your.message-unread.com/tw/px_mart/clean-back-doman-hk-php.php?lpkey=165952af33cd248519&domain=push.apush-link.click&uclick=7sqd37a2&uclickhash=7sqd37a2-7sqd37a2-b4u3-0-2ta8-slhe-9rsy-8a5447
your.message-unread.com 顯示
恭喜您! 您被電腦隨機選中!獲得免費領取Px mart超市禮券$10,000!
確定
親愛的用戶：
每個 星期四, 我們從台灣幸運用戶將會免費贏取Px mart 超市禮券$10,000 。
全聯福利中心
只需要在以下禮物中
找到一Px Mart禮券

假冒QR Code


府防疫政策實聯制
he government epidemic prevention measures,
tact-based registration policy
客進站乘車前及出站
描以下QRCode完成實
記，謝謝您的配合。
can the QR Code to complete the
ased Registration before and after
ney. Thank you for your coopera-
台灣高鐵
1922
訊息
今天 下午5:56
場所代碼：
1423218349653 12 本
次實聯簡訊限防疫目的
使用。
1423 2183 4965 312

假冒 QR Code

QR Code 真假？

惡意 QR Code

- 絕大多數的QR碼都是正常的，是企業用來和大眾互動的模式。但還是有惡意QR碼的存在，而且如果它們跟我們之前見過的其他類型垃圾郵件(SPAM)一樣的話，那可以預期的是它們只會越變越多。

非官方的App程式


iPhone
iPad
Android
游戏
精品推荐
热门网游
飙升
苹果榜
更多
赛尔号超级
嘉妃传-第..
武侠传奇
我的世界抽
王者荣耀：
口袋妖怪复
AppStore
Pokémon..
三国群英传
弹弹堂S-Q.
疯狂奔跑者
狩魔者2:新.
安魂曲
AppStore
狂暴之翼：
倩女幽魂-..
球球大作战
少年西游记
死神觉醒—
花千骨
软件
精品推荐
装机必备
飙升
苹果榜
更多
百度—最好
大众点评团
AppStore
天天私服-..
今日头条-..
爱奇艺视频
Next - Nu.

我們需要注意些什麼？

誘因

- 免費
- 色情
- 便利

裝置

- 程式來源
- 系統更新
- 要求權限
- 提示訊息
- 安全軟體

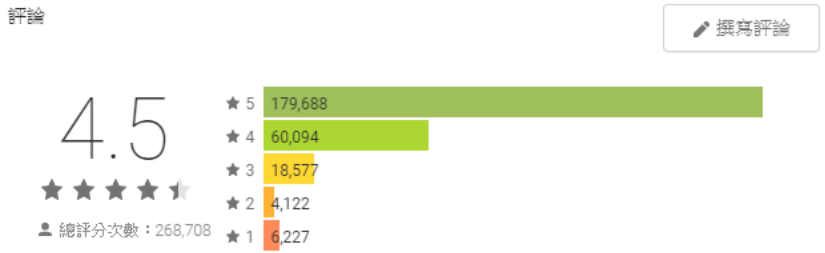
目的

- 帳號密碼
- 點選連結
- 下載其他程式

如何下載安全的軟體

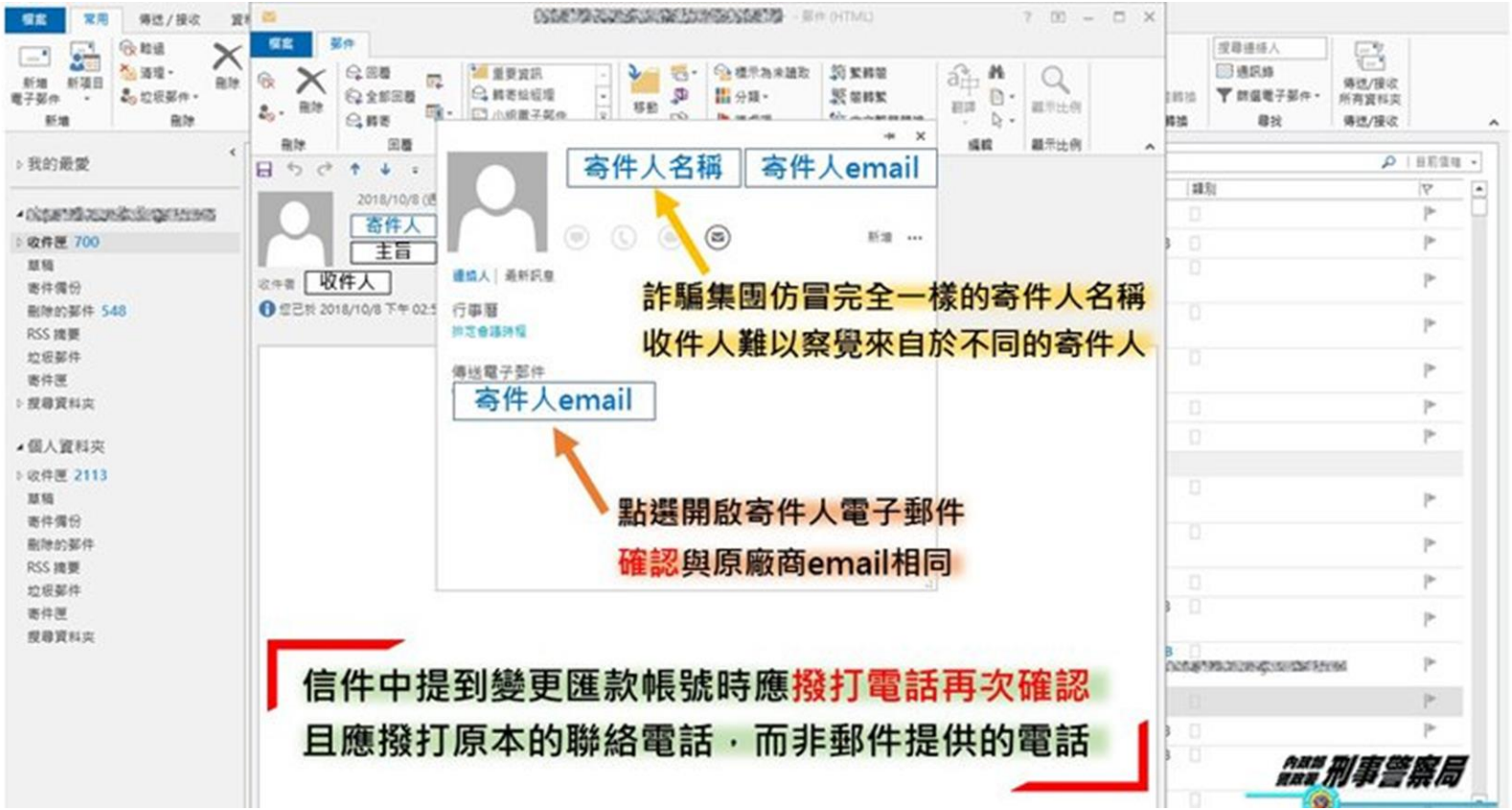
僅供參考，並非絕對

- 僅從google play下載
- 評價

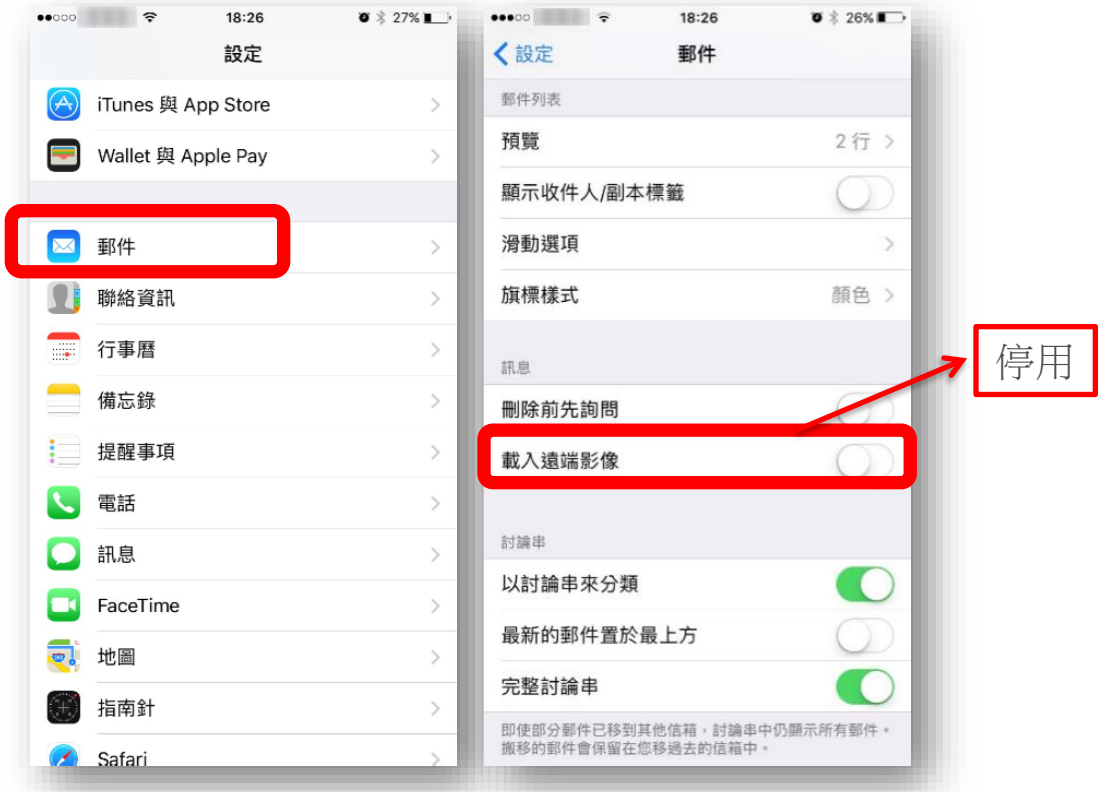


- 有無公司或提供者資訊是否有其他APP上架
- 安裝次數
- 知名廠商
- 問同事、朋友

郵件安全性

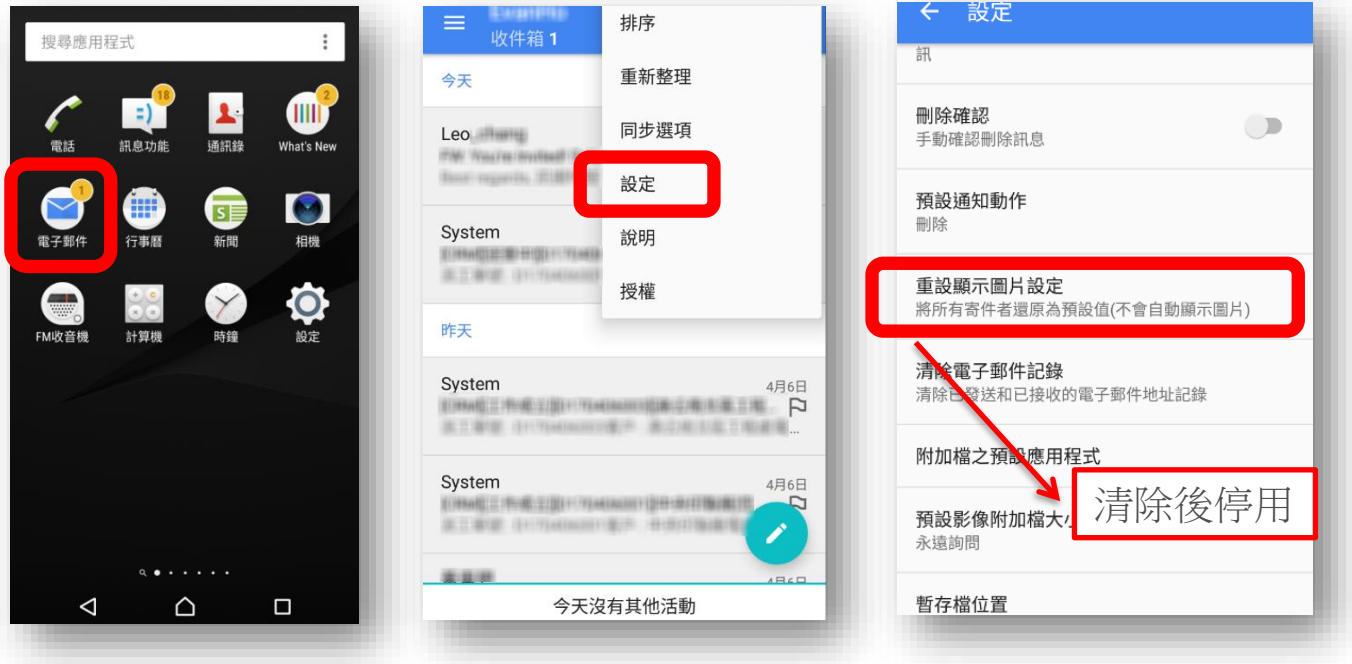

寄件人名稱
寄件人email
詐騙集團仿冒完全一樣的寄件人名稱
收件人難以察覺來自於不同的寄件人
寄件人email
點選開啟寄件人電子郵件
確認與原廠商email相同
信件中提到變更匯款帳號時應撥打電話再次確認
且應撥打原本的聯絡電話，而非郵件提供的電話
刑事警察局

iPhone 郵件安全性設定-停用自動顯示圖片



注意：IOS 手機停用郵件自動下載圖片的方法依各版本會有不同

Android 郵件安全性設定-停用自動顯示圖片



注意：Android 手機停用郵件自動下載圖片的方法依各廠牌手機及版本會有不同

落實行動裝置安全觀念

1. 密碼強度要夠
2. 不與他人共用私人手機
3. 只從官方來源取得App程式
4. 判斷App程式所要求的權限合理性
5. 仔細觀看所有的提示訊息
6. 遇到索取帳號密碼的情形時要特別提高警覺
7. 小心App中的指示（點連結、安裝其他App…）

落實帳號安全觀念


建立粉絲專
建立社團
新社團
建立廣告
在 Facebo
活動紀錄
動態消息
設定
登出
搜尋
首頁
尋找朋友
一般
帳號安全和登入
隱私
動態時報與標籤
封鎖
語言
臉部辨識
通知
行動版
公開的貼文
帳號安全和登入
你登入時所在的位置
Windows 電腦 · Taoyüan, Taiwan
Firefox · 目前在線上
Samsung Galaxy Note 5 · Taoyüan, Taiwan
Messenger · 17小時前
查看更多
不是你嗎？
登出

落實裝置安全觀念

利用暗藏惡意程式的盜版軟體或冒牌安裝程式來誘騙使用者下載

譬如使用者會去尋找一些提供「**有限免費版**」與「**完整付費版**」兩種版本的正版軟體的**破解版**

office 365免費破解 完整版 安裝和詳細信息

- 軟件名：office 365 完整版免費下載
- 下載文件大小：5.64MB
- 兼容性：window 64位/32位

如何安裝 office 365免費破解 完整版

- 使用WinRAR或WinZip或默認Windows命令提取壓縮文件。
- 解壓文件後請看說明,按照說明來安裝

office 365免費破解 完整版 下載

正版購買:前往

TeamViewer (远程软件)v15.27.3.0 无限制版

分享到：

软件大小：63.29 MB　　软件语言：简体中文

软件授权：破解版　　软件类别：网络共享

更新时间：2022-03-31　　官方网站：www.nokia88.com

应用平台：Win7,Win8,WinXP　　软件等级：

11.1%　　88.9%

网盘下载
需跳转网盘下载

安装破解教程

1、首先鼠标双击右键下载并解压软件压缩包，之后得到主程序及破解补丁，然后开始软件安装

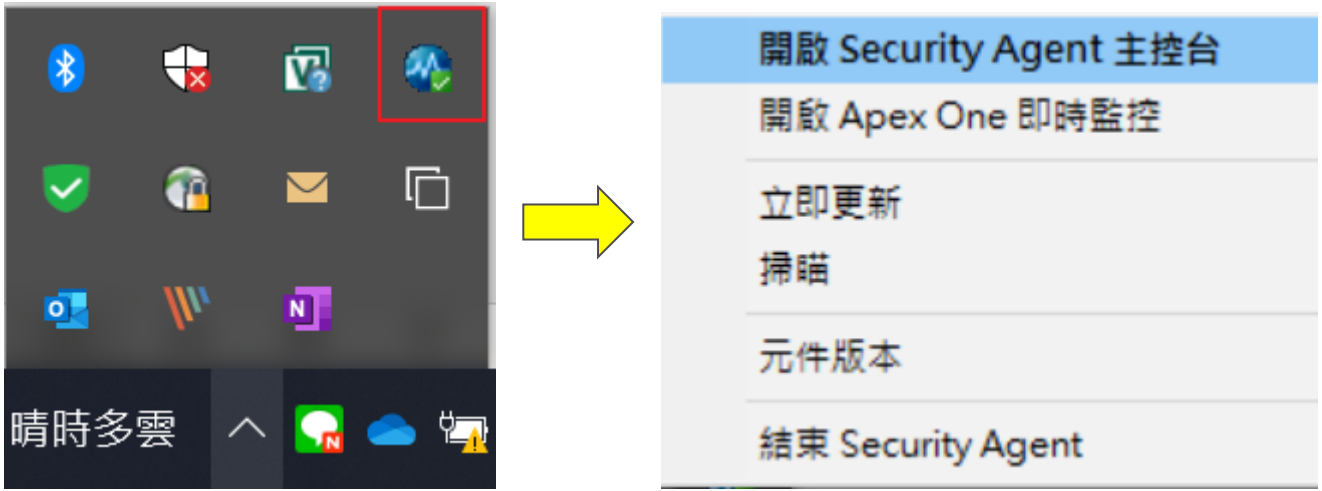
2、安装完成之后将破解补丁移动复制到软件安装目录下，默认路径为：C:\Program Files (x86)\TeamViewer，并选择双击打开

3、然后点击【应用】按钮，等待软件破解完成，提示成功，如下图所示：

ApexOne用户端介面

ApexOne用戶端介面

右下角圖示按右鍵選擇開啟Security Agent主控台



ApexOne用戶端介面

ApexOne用戶端介面

ApexOne用戶端介面

ApexOne用戶端介面

ApexOne用戶端介面

- [解除鎖定]用於啟動可能由管理員限制的所有功能。

ApexOne用戶端介面

- [元件版本]用於檢視用戶端版本、連線、元件等資訊

補充資料

- 網頁:
  - 官方網頁

    http://www.trendmicro.tw/
  - 下載專區

    http://downloadcenter.trendmicro.com/
  - 技術支援資料庫

    https://success.trendmicro.com/

Thank you!