

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

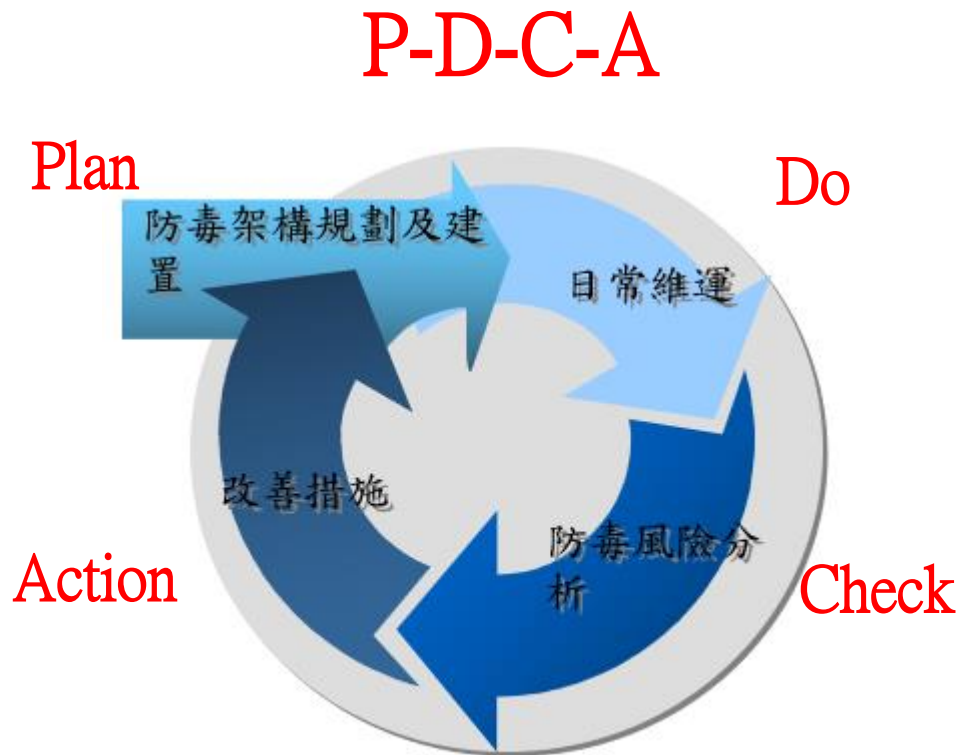
 - 勒索軟體防護與解密工具
 - 行動裝置安全與上網安全
- APEXONE用戶端畫面說明

ES0 服務

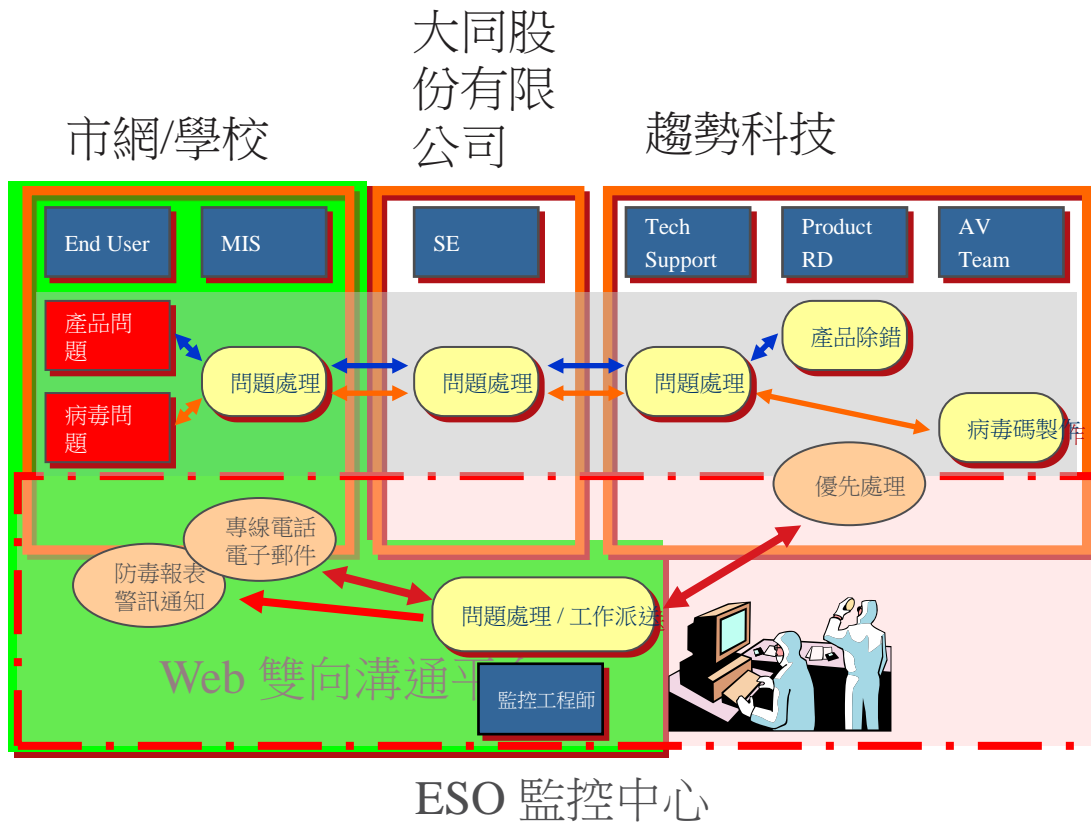
- 服務說明
 - 介面總覽
 - 病毒處理流程總覽
 - 病毒處理流程細項介紹
 - 其他說明
-

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



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



新北市教育研究發展中心

登出

首頁

諮詢服務 ▾

監控資訊 ▾

ESO ▾

客戶專屬 ▾

管理 ▾

資安情報

- 趨勢部落格
- 企業客戶電子報
- 毒賣新聞
- 趨勢科技認證中心

研究與報告

- 中文版資安威脅研究報告
- 漏洞

產品

- 安全威脅百科全書
- 病毒&威脅專區
- 產品技術支援
- 下載中心
- 支援規範

案件管理系統 (各校有專屬登入帳號)



新北市教育研究發展中心

退出

首頁 諮詢服務 監控資訊 ESO 客戶專屬 管理



申請服務

案件狀態

案件查詢

Securing Your Journey
to the Cloud

TRC 線上服務系統

產品問題

產品問題

病毒問題

樣本分析
郵件分析
網頁類別分析
病毒資訊需求
ATTK Log 分析
勒索病毒

連線事件問題

DD 事件通報
外部資安通報
連線中繼站 C&C
CallBack
Third Party Software
偵測

非技術問題

報表問題
連線問題
聯絡資訊變更
其他

地區: 新北市教研中心

聯絡人員:

電話: -

郵件:

部門:

問題主類: 產品 - Apex One

問題描述:

產品版本:

作業系統:

上傳檔案: 沒有選擇檔案

驗證碼:

1. 若有檔案需上傳，請將檔案壓縮成*.ZIP 檔案並且加上密碼 "novirus"
2. 檔案大小之限制為 5 MB, 若超過此大小，請於 <https://ftp.trendeso.com.tw> 上傳，
上傳帳號: upload 上傳密碼: trend
上傳完畢後，請務必於案件描述中告知壓縮檔案名稱，謝謝！

案件管理系統（各校有專屬登入帳號）

TREND MICRO TRC
Threat Response Center

首頁 | 諮詢服務 | 監控資訊 | ESO | 客戶專屬 | 管理

申請服務

案件狀態

案件查詢

未結案

案件編號	公司	聯絡人員	回報日期	狀態	回應時間
Q201301230028	新北市教研中心	陳明輝	2013-01-23 15:46	等待客戶回覆訊息	2013-02-04 13:32

案件查詢

2013/1/27 - 2013/2/5 案件查詢

案件編號	公司	聯絡人員	回報日期	狀態	回應時間
Q201301310038	新北市教研中心	陳明輝	2013-01-31 21:00	問題已解決	2013-02-01 11:23

防毒相關工具(Anti-Threat Toolkit)



新北市教育研究發展中心

- 首頁
- 諮詢服務 ▾
- 監控資訊 ▾
- ESO ▾
- 客戶專屬 ▾
- 管理 ▾

資安情報

- 趨勢部落格
- 企業客戶電子報
- 毒賣新聞
- 趨勢科技認證中心

專屬文件

ATTK

產品終止技術服務公告

產品

- 安全威脅百科全書
- 病毒&威脅專區
- 產品技術支援
- 下載中心
- 支援規範

防毒相關工具(ATTK)下載

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

產品/版本OfficeScan 10, Worry-Free Business Security (原CS/CSM for SMB) 8, Worry-Free Business Security (原CS/CSM for SMB) 7, [View More](#)

更新於: 2023/01/17

文章ID: 000228114

類別: 移除病毒 / 惡意軟體

評價: 0



You are viewing an archived article because the product(s) tagged is no longer supported or the information mentioned is already outdated.



需要其他協助?

[前往討論區發問](#)

本文對您是否有幫助?



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。

您可以使用趨勢科技 Anti-Threat Toolkit (ATTK) 進行全系統掃描並產生相關記錄檔，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。

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



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) 進行全系統掃描並產生相關記錄檔，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。

評語:

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)



- 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)

- 閱讀網頁上的授權協議後，點選【I Accept】開始下載工具。
- 如果出現儲存或執行的訊息視窗，請點選【儲存】。
- 請將工具儲存在桌面上。
- 用滑鼠點選兩下儲存在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：atk_ScanCleanOnline_gui_x86.exe



atk_ScanCleanOnline_gui_x86.exe

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

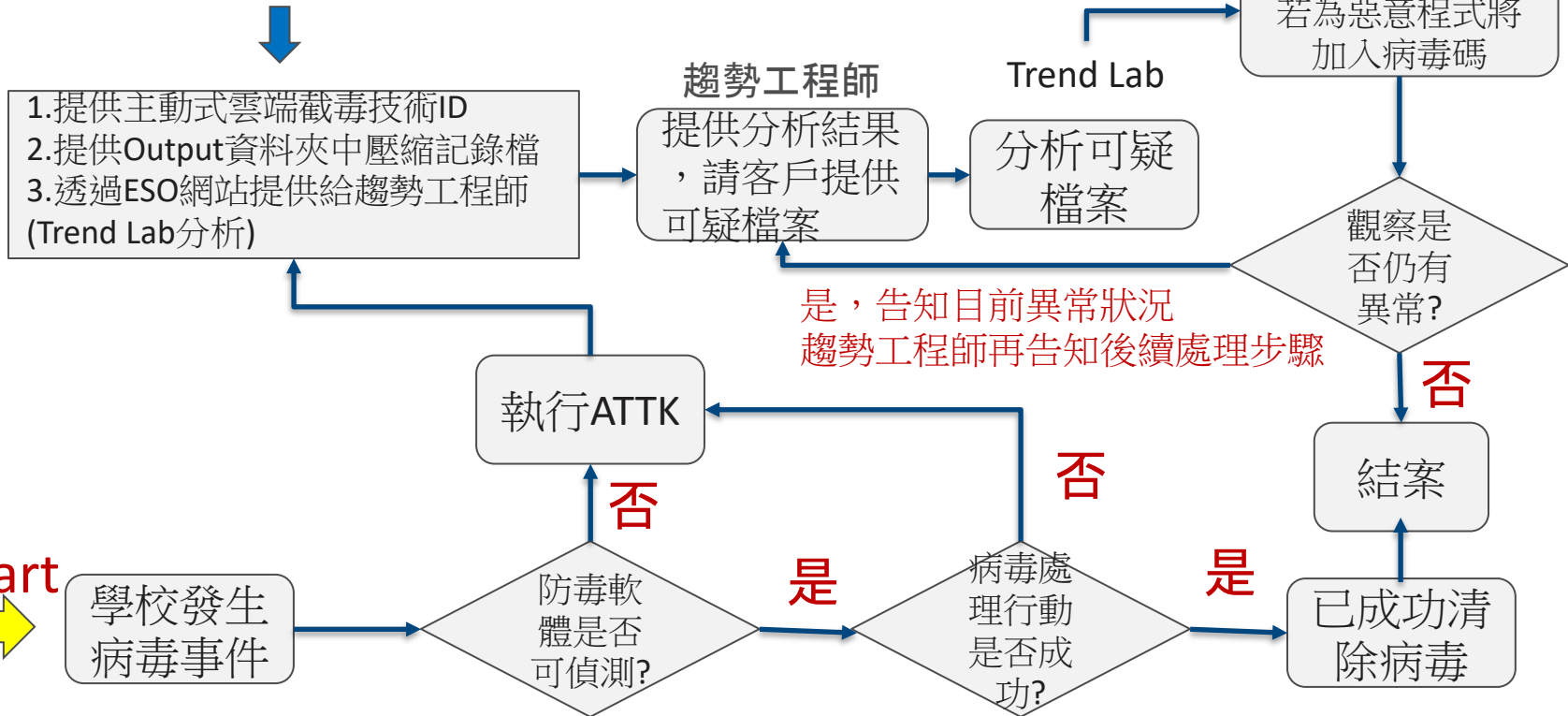
2. 學校應了解自身狀況

- 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

建立案件取得案件號碼



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ES0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)

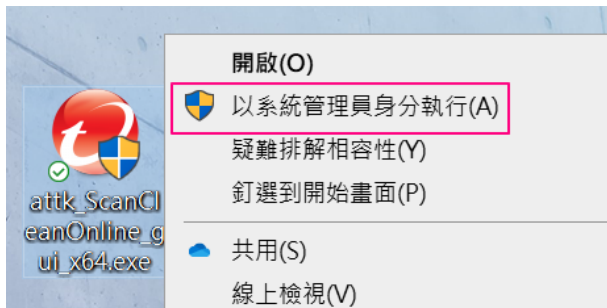
(2) 使用滑鼠點兩下attk_ScanXXX.exe, 程式會開始收集病毒相關資訊, 執行收集資訊期間會出現以下視窗, 請勿將其關閉

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。



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。



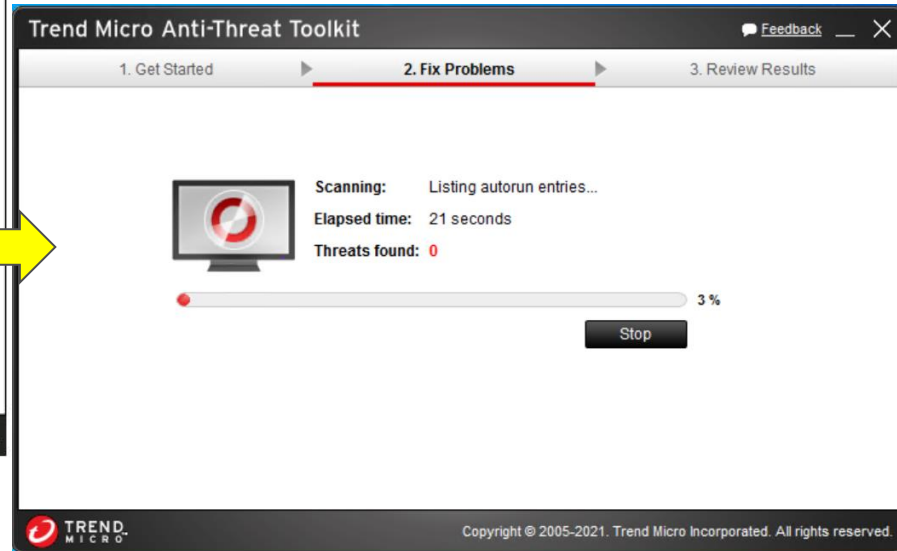
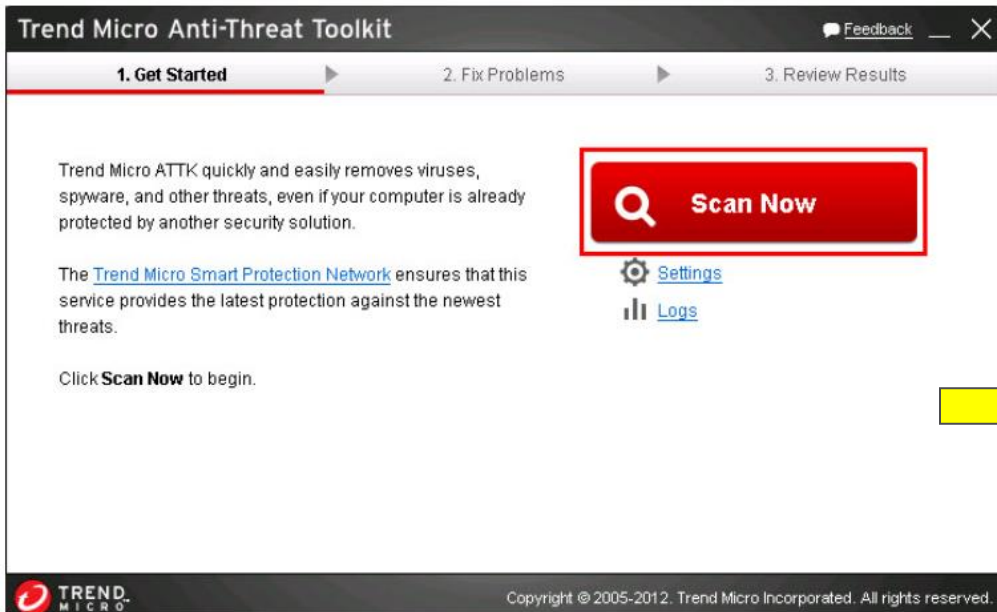
ATTK執行步驟

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。

```
C:\Users\Administrator\Desktop\attk_ScanCleanOnline_gui_x64 (1).exe
-----+
Anti-Threat Toolkit 1.2.62.1252
Copyright (c) 2021 Trend Micro Inc.
-----+
Starting...
Initializing...
Preparing components...
Initializing batcollector...
Running batcollector...
batCollector is starting @ 上午 09:31 - 2022/09/30 週五
FINDSTR: 無法開啟 ..\..\config.ini
batCollector is not enabled.
batCollector ended @ 上午 09:31 - 2022/09/30 週五
Collecting logs about batcollector...
Collecting suspect files from batcollector...
Initializing updater...
Running updater...
Collecting logs about updater...
```

ATTK執行步驟

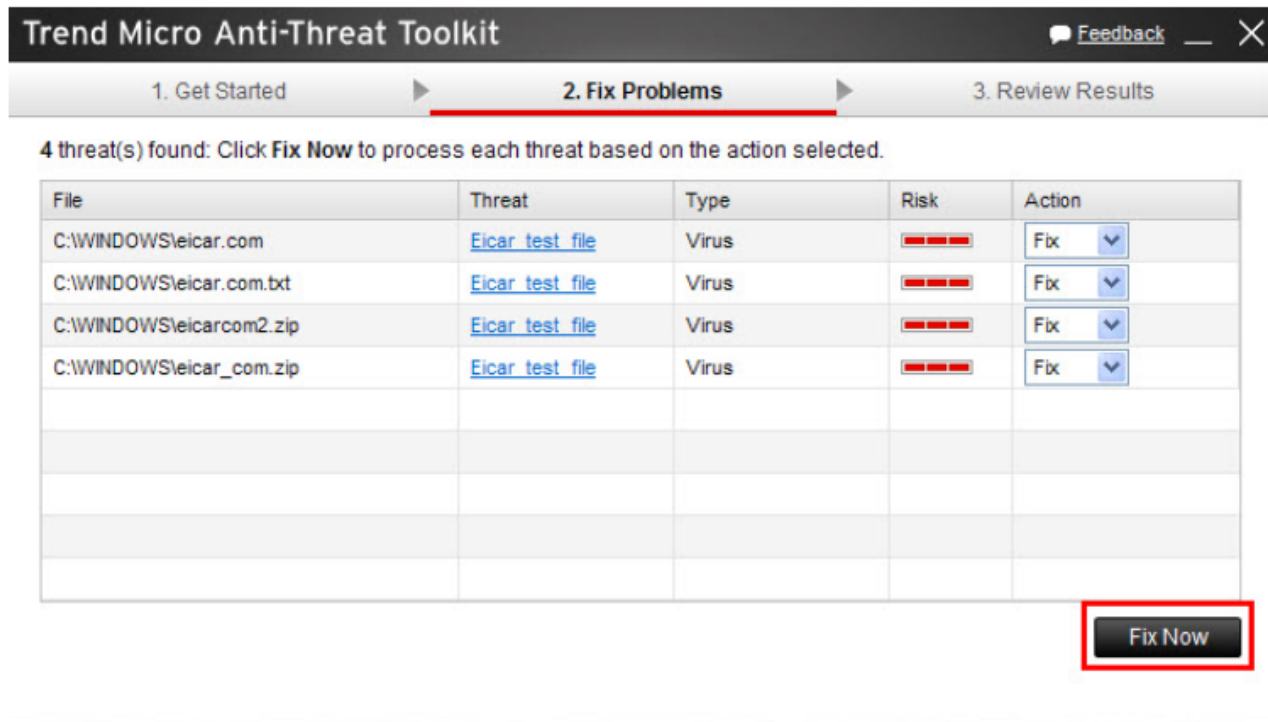
4. 出現TrendMicro AntiThreat Toolkit的視窗，請點選【Scan Now】開始進行掃描。



21 掃描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。



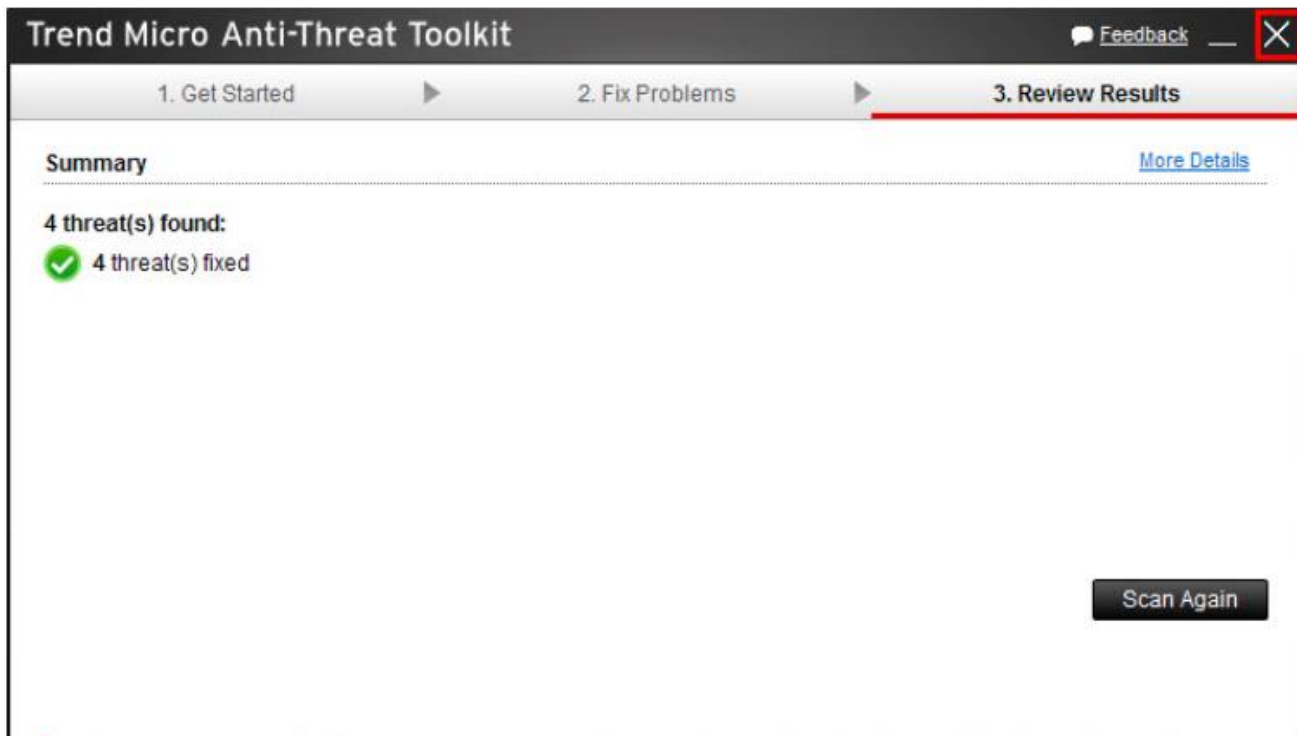
The screenshot shows the Trend Micro Anti-Threat Toolkit interface. At the top, there are three steps: 1. Get Started, 2. Fix Problems (highlighted with a red underline), and 3. Review Results. Below the steps, it says "4 threat(s) found: Click Fix Now to process each threat based on the action selected." A table lists the detected threats:

File	Threat	Type	Risk	Action
C:\WINDOWS\eicar.com	Eicar test file	Virus	High	Fix
C:\WINDOWS\eicar.com.txt	Eicar test file	Virus	High	Fix
C:\WINDOWS\eicarcom2.zip	Eicar test file	Virus	High	Fix
C:\WINDOWS\eicar_com.zip	Eicar test file	Virus	High	Fix

At the bottom right of the interface, there is a button labeled "Fix Now" which is highlighted with a red box.

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。

與趨勢科技技術支援團隊共享下列 ID 號碼，可讓他們自「主動式雲端載毒技術」擷取相關的資料。此 ID 號碼將在 7 天後到期。

主動式雲端載毒技術 ID

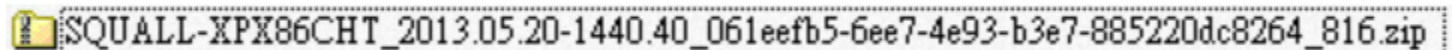
暫時 ID 號碼：3206

 TREND MICRO® SMART PROTECTION NETWORK™

「趨勢科技主動式雲端載毒技術」是新一代的雲端用戶端內容安全基礎結構，旨在提供主動式安全防護，保護客戶免於最新安全威脅的侵襲。進一步瞭解 [Learn more](#)

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。



SQUALL-XPX86CHT_2013.05.20-1440.40_061eefb5-6ee7-4e93-b3e7-885220dc8264_816.zip

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



新北市教育研究發展中心

首頁	諮詢服務 ▾	監控資訊 ▾	ESO ▾	客戶專屬 ▾	管理 ▾
----	--------	--------	-------	--------	------

申請服務

案件狀態

案件查詢

產品問題

產品問題

病毒問題

樣本分析

郵件分析

網頁類別分析

病毒資訊需求

ATTK Log 分析

勒索病毒

連線事件問題

DD 事件通報

外部資安通報

連線中繼站 C&C

CallBack

Third Party Software 偵測

非技術問題

報表問題

連線開通問題

聯絡資訊變更

* 廠區	新北市教研中心 ▾
* 聯絡人員	<input type="text"/>
* 電話	<input type="text"/> - <input type="text"/>
* 郵件	<input type="text"/>
部門	<input type="text"/>
問題主類	病毒 ▾ - Log Analysis ▾
問題描述	<div style="border: 1px solid gray; padding: 5px; min-height: 100px;"><p>電腦名稱： 電腦IP： 異常狀況或分析原因：</p></div> <p>1. 請提供用戶端偵測紀錄或通報資訊，有利於Log分析。 2. 若未提供該資訊，將會造成分析時間延長，敬請見諒！</p>
Log上傳	<input type="button" value="選擇檔案"/> 沒有選擇檔案
偵測紀錄/通報	<input type="button" value="選擇檔案"/> 沒有選擇檔案
驗證碼	 <input type="text"/>

送出聯絡問題

1. 若有檔案需上傳，請將檔案壓縮成 *.ZIP 檔案並且加上密碼 "virus"

2. 檔案大小之限制為 5 MB ,若超過此大小,請透過以下URL 上傳 <http://ftp.trendeso.com.tw/>,

帳號：upload 密碼：trend

上傳完畢後，請務必於案件描述中告知壓縮檔案名稱，謝謝！

病毒處理流程細項介紹 - 如何提交 病毒樣本



新北市教育研究發展中心

首頁 諮詢服務 ▾ 監控資訊 ▾ ESO ▾ 客戶專屬 ▾ 管理 ▾



Securing Your Journey
to the Cloud

TRC 線上服務系統

產品問題

產品問題

病毒問題

樣本分析

郵件分析

網頁類別分析

病毒資訊需求

ATTK Log 分析

勒索病毒

連線事件問題

DD 事件通報

外部資安通報

連線中繼站 C&C

CallBack

Third Party Software

偵測

非技術問題

* 廠區

* 聯絡人員

* 電話 -

* 郵件

部門

問題主類

問題描述

上傳樣本 沒有選擇檔案

驗證碼 

1. 若有檔案需上傳，請將檔案壓縮成*.ZIP 檔案並且加上密碼 "virus"
2. 檔案大小之限制為 5 MB,若超過此大小，請透過以下URL 上傳
<http://ftp.trendeso.com.tw/>

帳號：upload 密碼：trend

上傳完畢後，請務必於案件描述中告知壓縮檔案名稱，謝謝！



病毒處理流程細項介紹 - 如何提交 郵件分析



新北市教育研究發展中心

登出

首頁

諮詢服務 ▾

監控資訊 ▾

ESO ▾

客戶專屬 ▾

管理 ▾



Securing Your Journey
to the Cloud

TRC 線上服務系統

產品問題

產品問題

病毒問題

樣本分析

郵件分析

網頁類別分析

病毒資訊需求

ATTK Log 分析

勒索病毒

連線事件問題

DD 事件通報

外部資安通報

連線中繼站 C&C

CallBack

* 廠區	<input type="text" value="新北市教研中心"/>
* 聯絡人員	<input type="text"/>
* 電話	<input type="text"/> - <input type="text"/>
* 郵件	<input type="text"/>
部門	<input type="text"/>
問題主類	<input type="text" value="病毒"/> - <input type="text" value="Spam & Phishing Submit"/>
問題描述	<input type="text"/>
郵件樣本上傳	<input type="text" value="選擇檔案"/> 未選擇任何檔案

1. 若有檔案需上傳，請將檔案壓縮成 *.ZIP 檔案並且加上密碼 "virus"
2. 檔案大小之限制為 5 MB, 若超過此大小，請於 <https://ftp.trendeso.com.tw> 上傳，

上傳帳號：upload 上傳密碼：trend

上傳完畢後，請務必於案件描述中告知壓縮檔案名稱，謝謝！

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。

Copyright (c) 1989-2022 Trend Micro Incorporated. All rights reserved. [法律聲明與隱私權政策](#)

病毒處理流程細項介紹 - 如何提交 網頁類別分析-1



新北市教育研究發展中心

登出

首頁 諮詢服務 監控資訊 ESO 客戶專屬 管理



Securing Your Journey
to the Cloud

TRC 線上服務系統

產品問題

產品問題

病毒問題

樣本分析

郵件分析

網頁類別分析

病毒資訊需求

ATTN Log 分析

勒索病毒

連線事件問題

DD 事件通報

外部資安通報

連線中繼站 C&C

CallBack

Third Party Software

偵測

非技術問題

報表問題

連線開通問題

聯絡資訊變更

...

* 廠區

* 聯絡人員

* 電話 -

* 郵件

部門

問題主類 -

問題描述

網頁

網頁

網頁

網頁

檔案

未選擇任何檔案

1. 當URL於目前趨勢產品無法偵測或類型判斷錯誤，可透過此類別提供，若超過五個URL，可將URL貼至文字檔或是Excel提供分析，也可先透過以下Site Safety Center網站進行判別

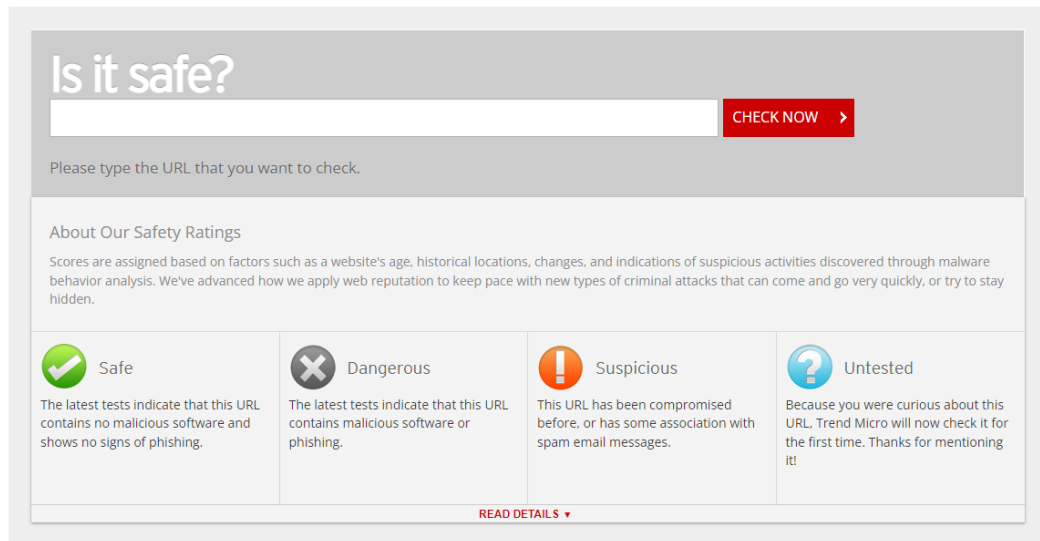
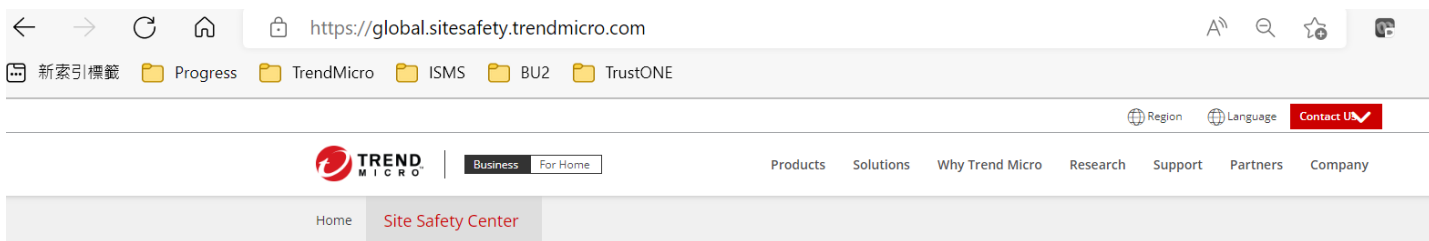
<https://global.sitesafety.trendmicro.com/>

2. 當您提供相關URL時，請您將http或https修改成hxxp或hxxps

3. 請將文字檔壓縮成*.ZIP檔案並且加上密碼"virus"



病毒處理流程細項介紹 - 如何提交 網頁類別分析-2







Is it safe?

[CHECK NOW](#)

Please type the URL that you want to check.

About Our Safety Ratings

Scores are assigned based on factors such as a website's age, historical locations, changes, and indications of suspicious activities discovered through malware behavior analysis. We've advanced how we apply web reputation to keep pace with new types of criminal attacks that can come and go very quickly, or try to stay hidden.

 Safe The latest tests indicate that this URL contains no malicious software and shows no signs of phishing.	 Dangerous The latest tests indicate that this URL contains malicious software or phishing.	 Suspicious This URL has been compromised before, or has some association with spam email messages.	 Untested Because you were curious about this URL, Trend Micro will now check it for the first time. Thanks for mentioning it!
---	--	--	---

[READ DETAILS](#)

病毒處理流程細項介紹 - 如何提交 其他病毒問題



新北市教育研究發展中心

首頁 諮詢服務 監控資訊 ESO 客戶專屬 管理



Securing Your Journey
to the Cloud

TRC 線上服務系統

產品問題

產品問題

病毒問題

樣本分析
郵件分析
網頁類別分析
病毒資訊需求
ATTK Log 分析
勒索病毒

連線事件問題

DD 事件通報
外部資安通報
連線中繼站 C&C
CallBack
Third Party Software
偵測

非技術問題

* 廠區	<input type="text" value="新北市教研中心"/>
* 聯絡人員	<input type="text"/>
* 電話	<input type="text"/> - <input type="text"/>
* 郵件	<input type="text"/>
部門	<input type="text"/>
問題主類	<input type="text" value="病毒"/> <input type="text" value="勒索病毒"/>
問題描述	<input type="text"/>
Log上傳	<input type="button" value="選擇檔案"/> 沒有選擇檔案
驗證碼	 <input type="text"/>
	送出服務問題

避免開啟未經確認的電子郵件或者點選郵件當中的連結，這類連結一旦點選就會啟動勒索病毒安裝程序。

備份您的重要檔案，遵守 3-2-1 原則：3 份備份、2 種儲存媒體、1 個不同的存放地點。

定期更新系統、軟體及應用程式，讓您的應用程式隨時保持最新狀態，防堵最新的漏洞。

相關資訊可點選 [趨勢Blog](#)

相關資料也可參考TRC Portal → ESO → ESO技術支援 → 勒索病毒相關文件

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)

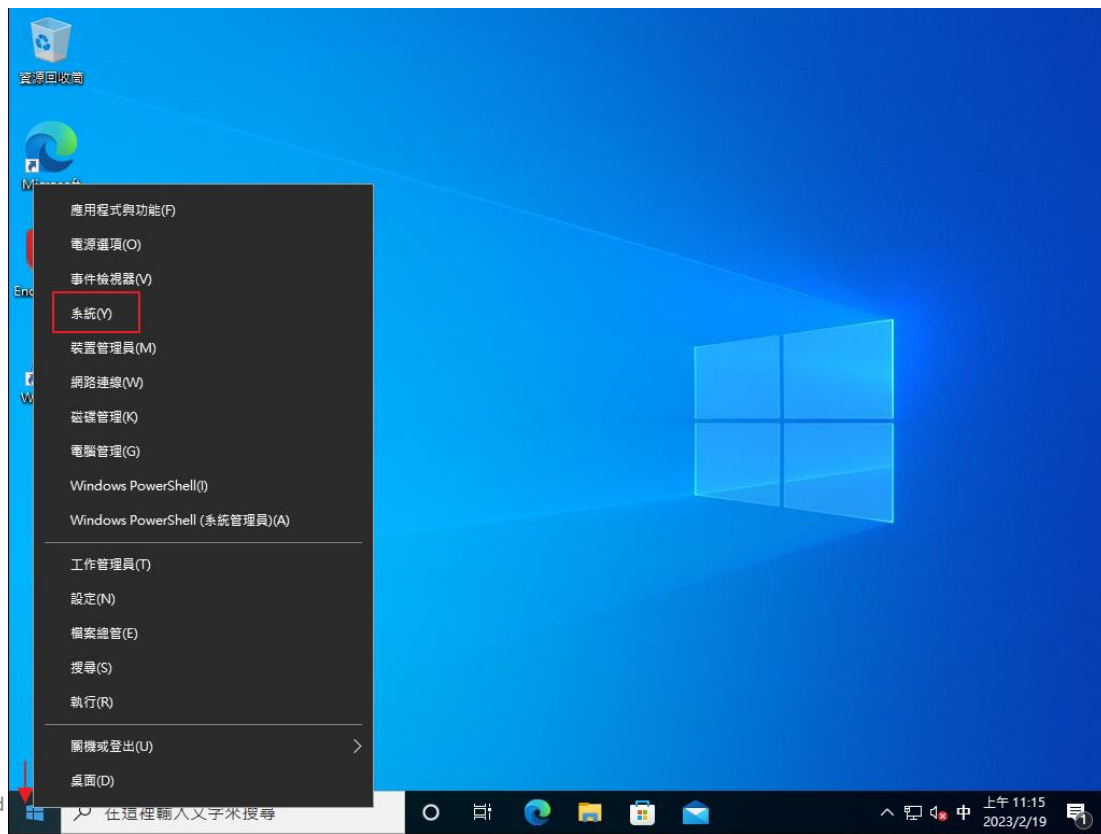
Domain name < -學校名稱

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]

The screenshot shows the Windows Settings application. On the left is a navigation pane with categories like 'System', 'Display', 'Sound', etc. The main area is titled '關於' (About) and contains system information. A red box highlights the '重新命名此電腦' (Rename this PC) link at the bottom of the system specifications section.

設定

首頁

尋找設定

系統

- 顯示器
- 音效
- 通知與動作
- 專注輔助
- 電源與睡眠
- 儲存空間
- 平板電腦模式
- 多工
- 投影到此電腦
- 共用體驗
- 剪貼簿

關於

系統正在監控並保護您的電腦。

- ✓ 病毒與威脅防護
- ✗ 防火牆與網路保護
- ▲ 應用程式與瀏覽器控制
- ✓ 帳戶防護
- ✓ 裝置安全性

[參閱 Windows 安全性中的詳細資訊](#)

裝置規格

裝置名稱	DESKTOP-QOKT2BA
處理器	Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz 2.20 GHz
已安裝記憶體(RAM)	4.00 GB
裝置識別碼	4D06F52E-BC3D-462B-A725-BF86BF586086
產品識別碼	00331-10000-00001-AA287
系統類型	64 位元作業系統, x64 型處理器
手寫筆與觸控	此顯示器不提供手寫筆或觸控式輸入功能

重新命名此電腦

下午 11:21
2023/2/19

- 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。

重新命名電腦

重新命名電腦

您可以使用字元、連字號與數字的組合。

目前的電腦名稱: DESKTOP-QOKT2BA

下一步

取消

重新命名電腦

重新命名電腦

重新啟動之後，電腦名稱將變更為: ntpc-XXX

立即重新啟動

稍後重新啟動

- 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。



The screenshot shows the Windows Settings application. On the left is a navigation pane with categories like 'System', 'Display', 'Sound', etc. The 'System' category is selected. The main area is titled '關於' (About) and contains a status message, security status indicators, and system specifications. A red box highlights the '裝置名稱' (Device name) field, which contains 'ntpc-XXX'. Below the specifications is a button labeled '重新命名此電腦' (Rename this PC).

設定

🏠 首頁

🔍 尋找設定

系統

🖥️ 顯示器

🔊 音效

🗨️ 通知與動作

🌙 專注輔助

🔌 電源與睡眠

💾 儲存空間

📱 平板電腦模式

🛠️ 多工

📺 投影到此電腦

🌐 共用體驗

📄 剪貼簿

關於

系統正在監控並保護您的電腦。

- ❌ 防火牆與網路保護
- ⚠️ 應用程式與瀏覽器控制
- ✅ 帳戶防護
- ✅ 裝置安全性

[參閱 Windows 安全性中的詳細資訊](#)

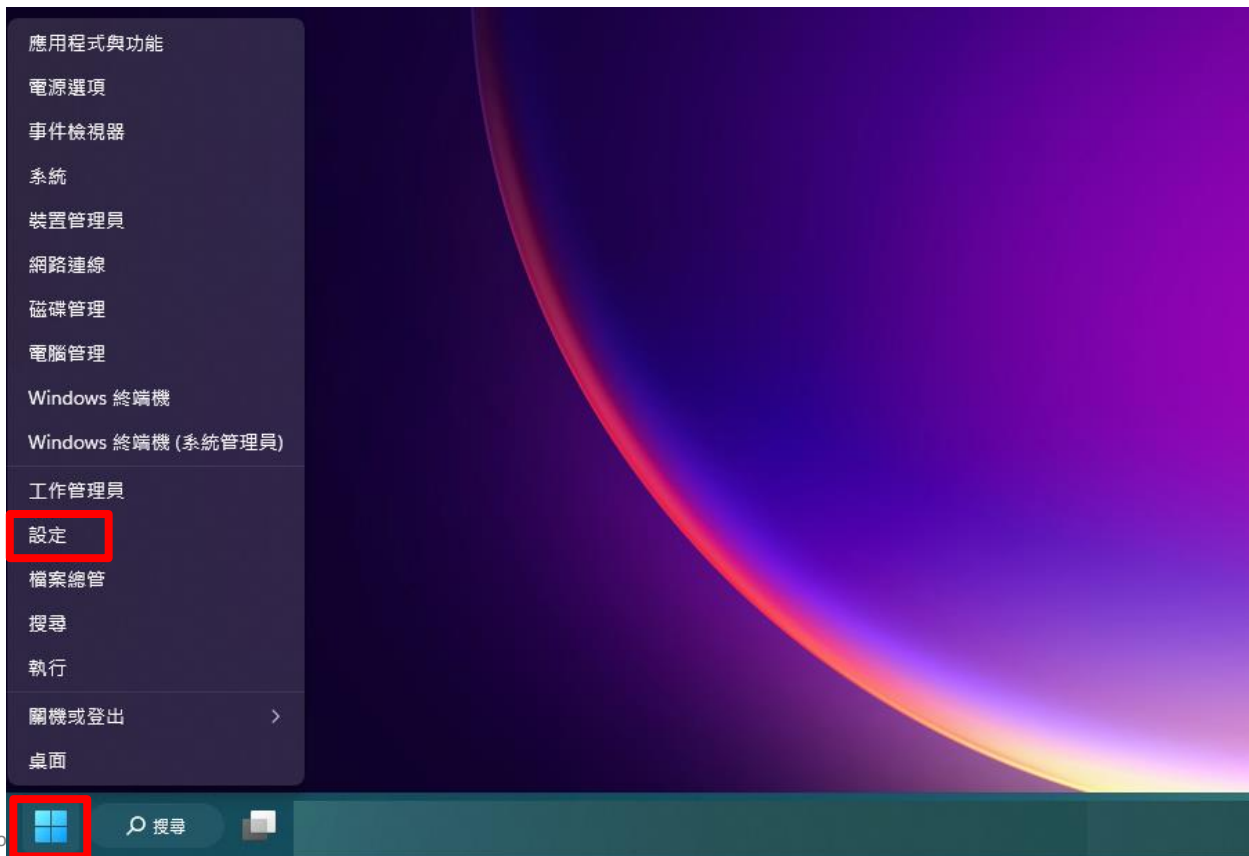
裝置規格

裝置名稱	ntpc-XXX
處理器	Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz 2.20 GHz
已安裝記憶體(RAM)	4.00 GB
裝置識別碼	4D06F52E-BC3D-462B-A725-BF86BF586086
產品識別碼	00331-10000-00001-AA287
系統類型	64 位元作業系統, x64 型處理器
手寫筆與觸控	此顯示器不提供手寫筆或觸控式輸入功能

重新命名此電腦

如何修改/確認電腦的名稱-Windows 11

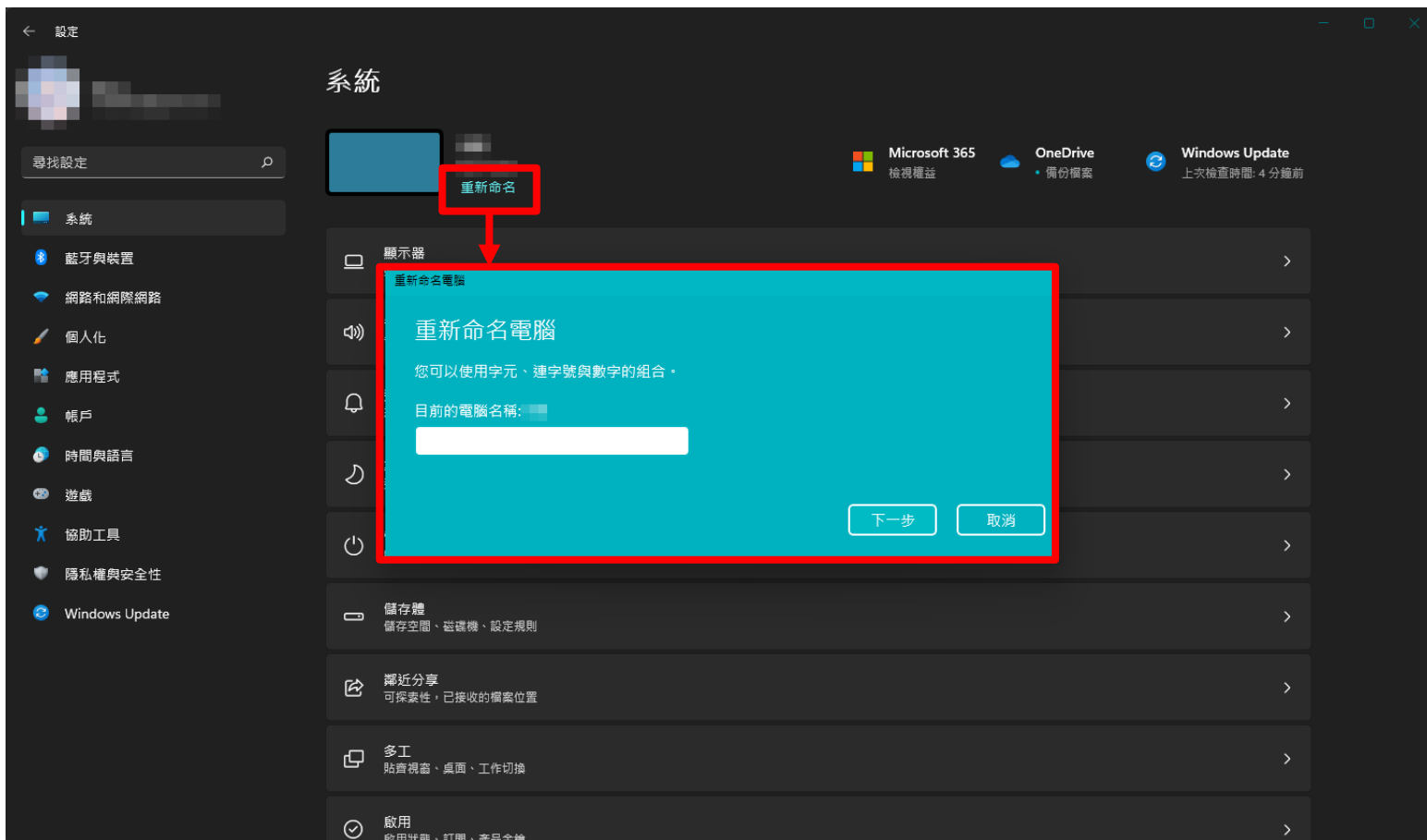
- 左下角開始圖示按右鍵點[設定]



- 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]。



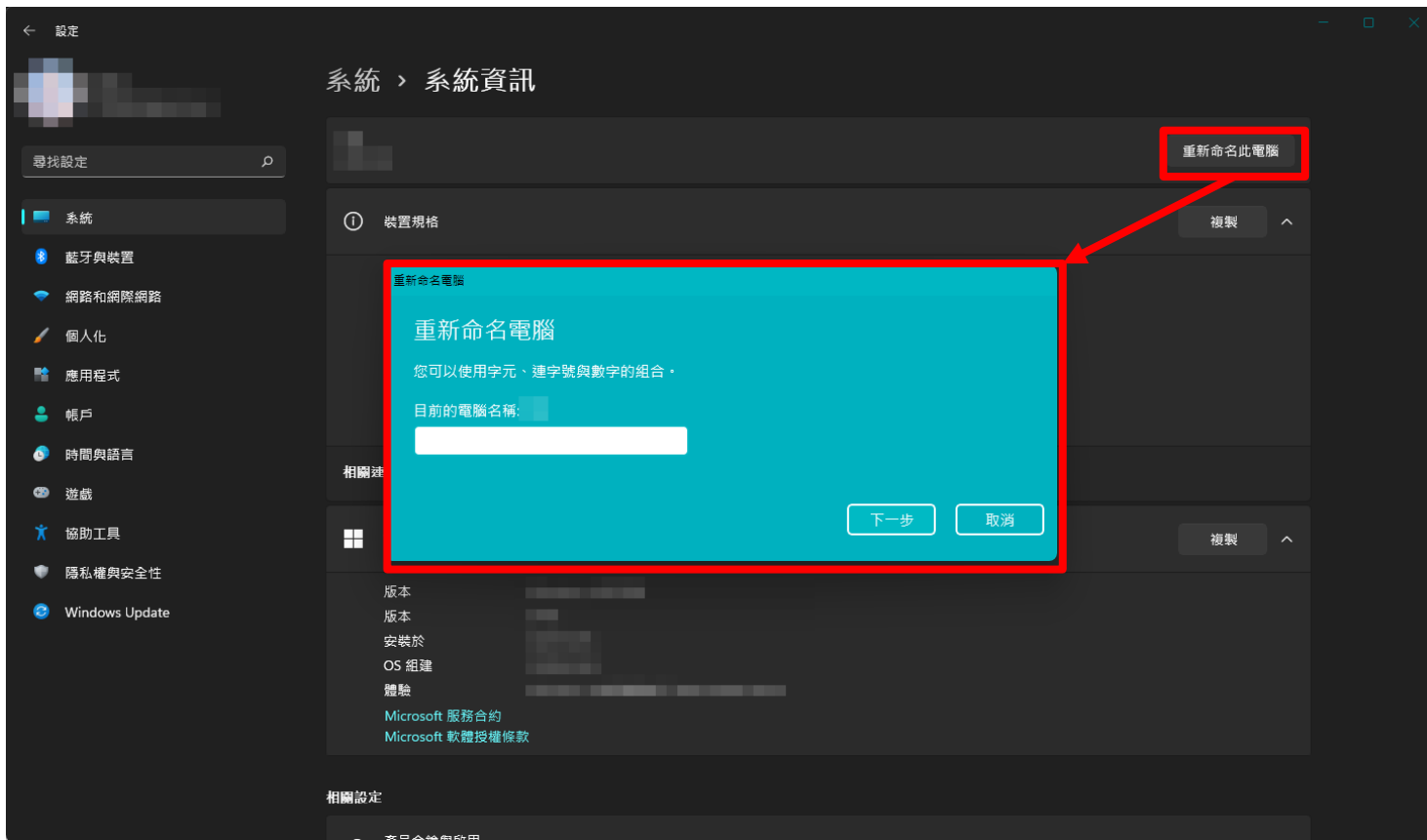
- 或是在[系統]頁面中，選擇最下方的[系統資訊]。



- [系統資訊]的頁面右上方， 點擊[重新命名此電腦的]。



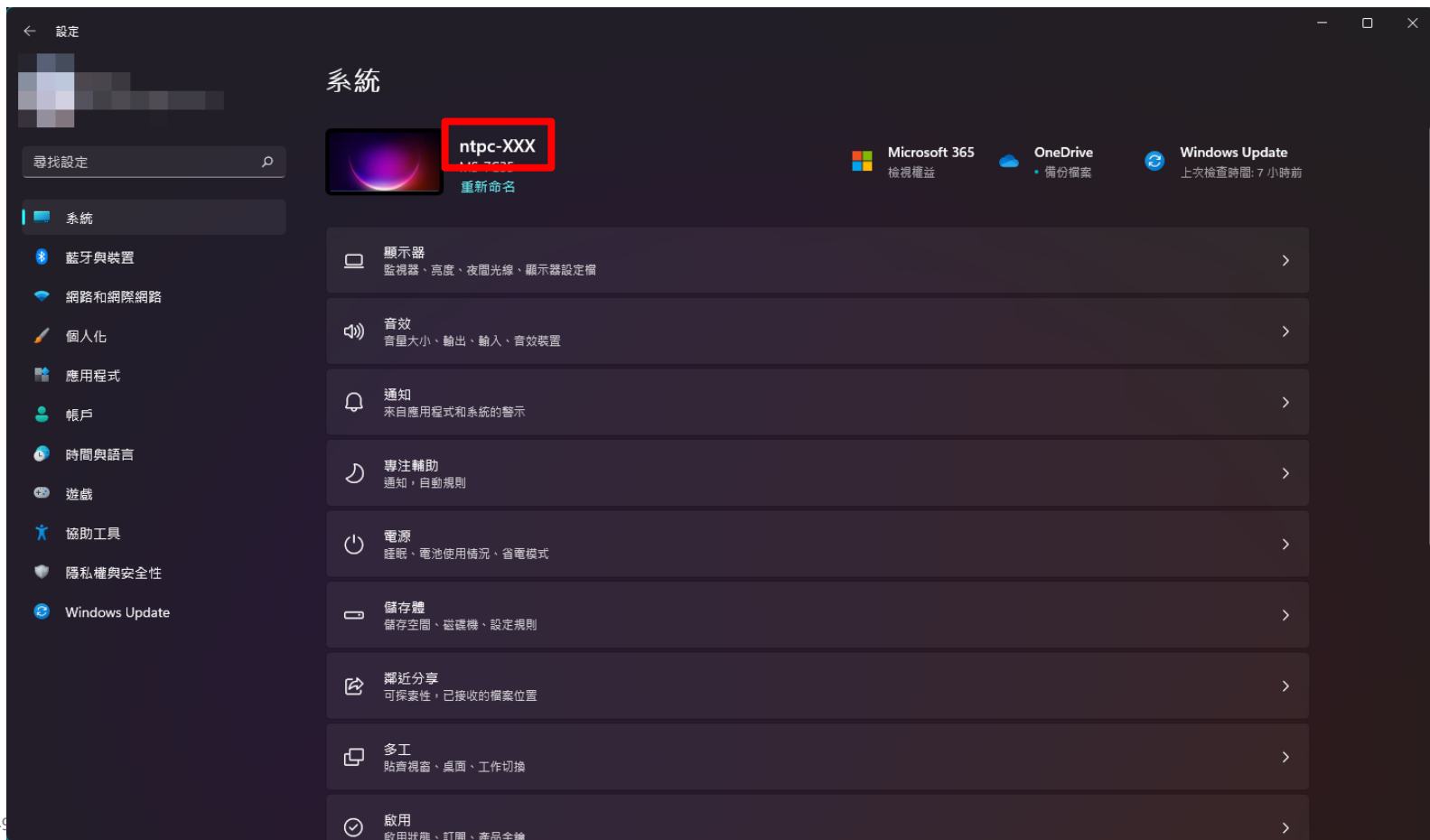
- 輸入名稱後，點選[下一步]。



- 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/>

The screenshot shows the Trend Micro Apex One console interface. At the top, the browser address bar displays the URL: <https://osce.ntpc.edu.tw/officescan/console/html/cgi/cgiChkMasterPwd.exe>. The page header includes the Trend Micro logo and the text "Trend Micro Apex One™" on the left, and a link "取得說明" on the right. The main content area is divided into two sections. On the left, under the heading "登入" (Login), there are three input fields: "使用者名稱:" (Username) with the placeholder "輸入使用者名稱", "密碼:" (Password) with the placeholder "輸入密碼", and "網域:" (Domain) with an empty field. Below these fields is a red "登入" button and a link "為使用者提供用戶端安裝程式" (Provide client installation program for users). A yellow arrow points from this link to the right section. The right section is titled "MSI 用戶端安裝" (MSI Client Installation) and contains a numbered list of instructions: 1. 請點選下面其中一個按鈕，下載 Apex One Security Agent 32 位元或 64 位元 MSI 安裝套件。 (Click one of the buttons below to download the Apex One Security Agent 32-bit or 64-bit MSI installation package.) 2. 完成下載後，執行 MSI 套件。 (After downloading is complete, run the MSI package.) 3. 請點選「開始」。 (Click "Start"). 4. 請點選「下一步」以安裝 Apex One Security Agent。 (Click "Next" to install the Apex One Security Agent.) At the bottom of this section are two blue buttons: "立即下載 32 位元套件" (Download 32-bit package immediately) and "立即下載 64 位元套件" (Download 64-bit package immediately).

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

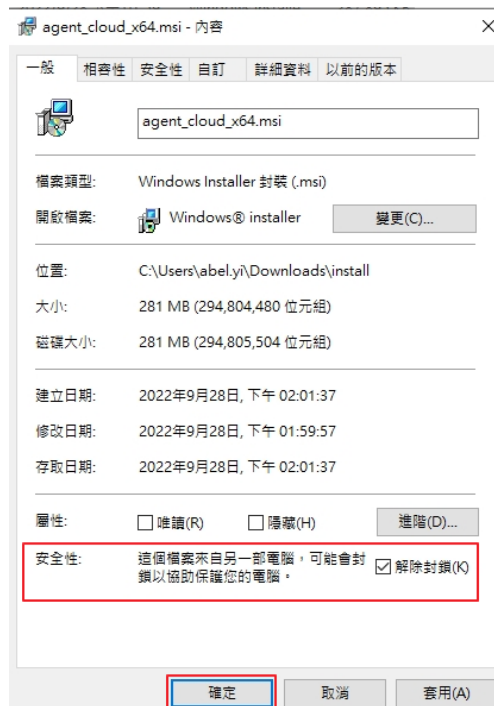
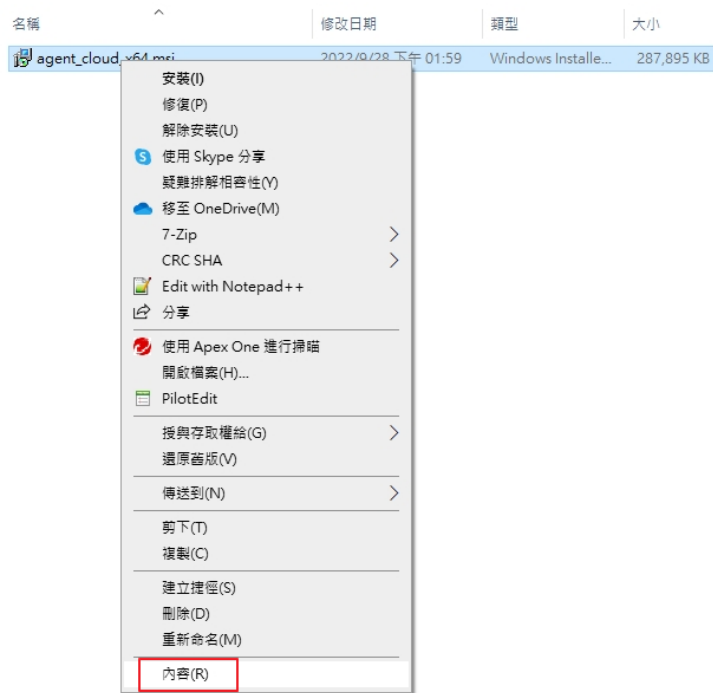
用戶端程式安裝方式- Internal Web Page(1)

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」。



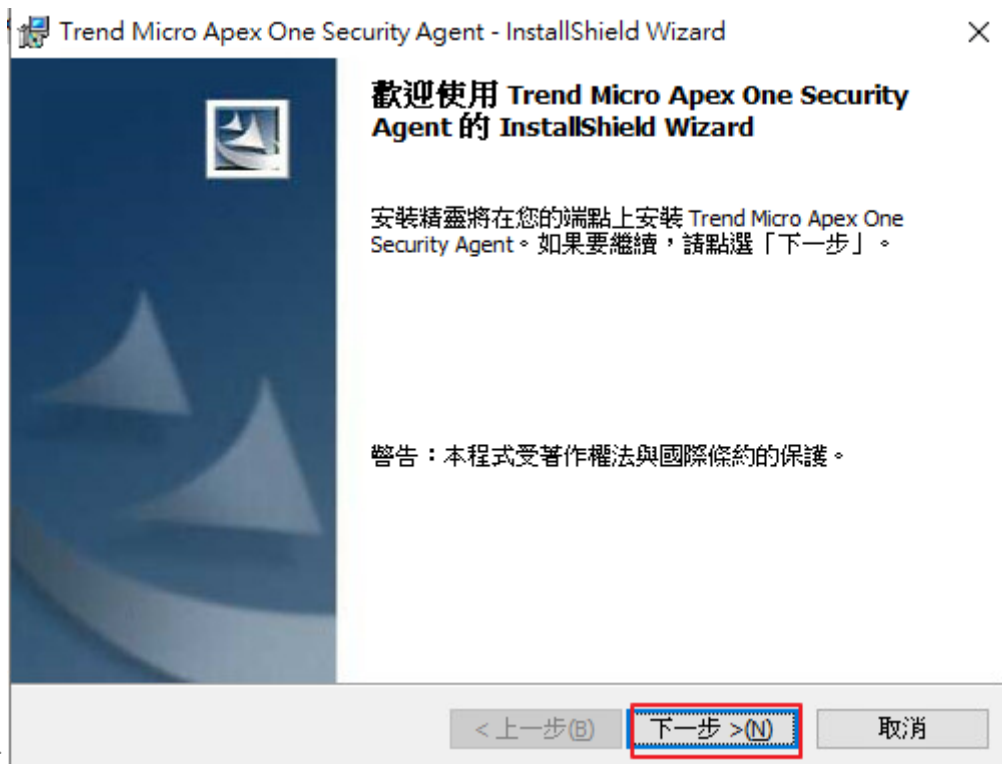
用戶端程式安裝方式- Internal Web Page(2)

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」。



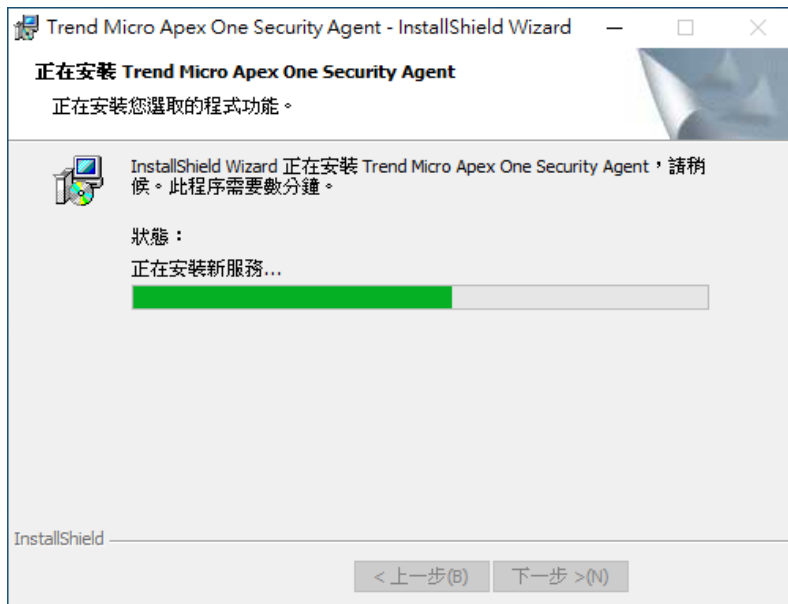
用戶端程式安裝方式- Internal Web Page(3)

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。



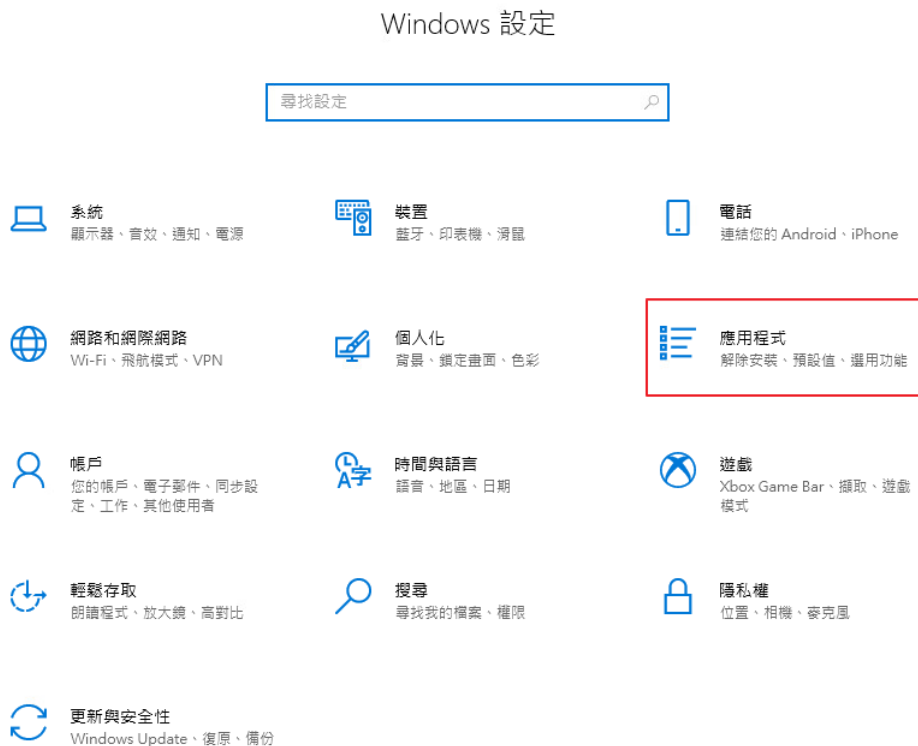
用戶端程式安裝方式- Internal Web Page(7)

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」

The screenshot shows the Windows Settings application, specifically the 'Apps & Features' section. The left sidebar is visible, showing navigation options like 'Settings', 'Home', 'Search Settings', 'Apps', 'App Features', 'Pre-installed Apps', 'Offline Maps', 'Open Websites with Apps', 'Video Playback', and 'Start'. The main area is titled '應用程式與功能' (Apps & Features) and lists several installed applications. The 'Trend Micro Apex One Security Agent' is highlighted with a red box. Below its name, the version '14.0.11092' and the date '2022/8/17' are shown. At the bottom of this entry, there are two buttons: '修改' (Modify) and '解除安裝' (Uninstall). A yellow arrow points from the '解除安裝' button to a larger, semi-transparent dialog box that appears over the list. This dialog box contains the text '將解除安裝此應用程式與其相關資訊。' (Remove this app and its related info.) and a red-bordered button labeled '解除安裝' (Uninstall).

Application Name	Company	Size	Date	Actions
Microsoft Visual C++ 2015-2019 Redistributable (...)		22.0 MB	2022/8/17	
Microsoft Visual C++ 2015-2019 Redistributable (...)		19.7 MB	2022/8/17	
Office	Microsoft Corporation	112 KB	2022/8/17	
OneNote	Microsoft Corporation			
Skype	Skype			
Sticky Notes	Microsoft Corporation			
Trend Micro Apex One Security Agent			2022/8/17	修改 解除安裝
WebP 影像延伸模組	Microsoft Corporation	8.00 KB	2022/8/17	
Xbox	Microsoft Corporation	16.0 KB	2022/8/17	

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)



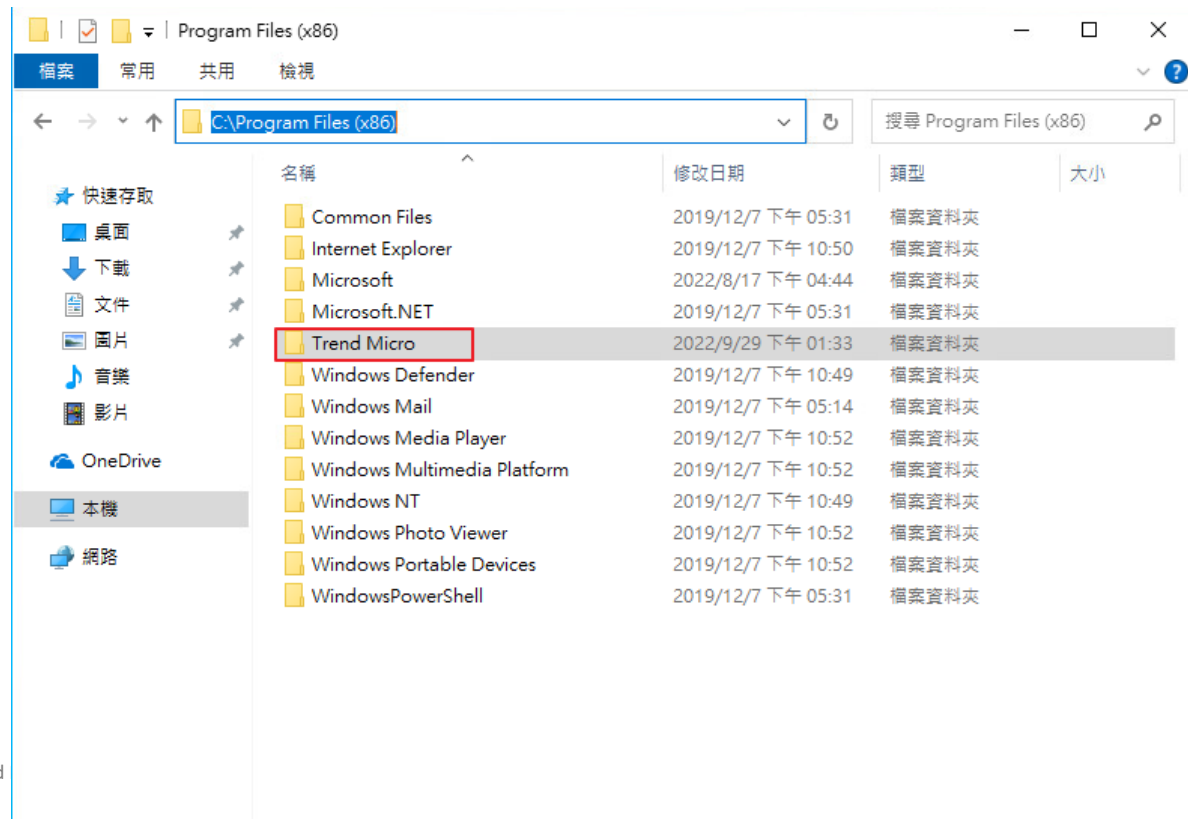
用戶端程式移除方式-(4)

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	<ol style="list-style-type: none">1.事實發生日:111/12/012.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/ 林妍濤 | 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

ASUSTOR Inc. 華芸科技
粉絲專頁 · 3 小時 ·

⚠️ Deadbolt勒索軟體排除步驟 ⚠️

如果被勒索軟體綁架，該如何處理？

https://www.asustor.com/knowledge/detail?id=6&group_id=630

因應這次Deadbolt 勒索軟體事件，為盡速將被攻擊的NAS排除勒索軟體，我們已針對不同的狀況擬定排除步驟，請您依照實際的狀況參考上方的連結進行。

對應日益猖獗的各式勒索軟體，ASUSTOR 未來仍會持續監控任何潛在危害及攻擊，加強網路安全防禦，不斷提供更高安全性的儲存解決方案，以共同維護資料及網路的安全。



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



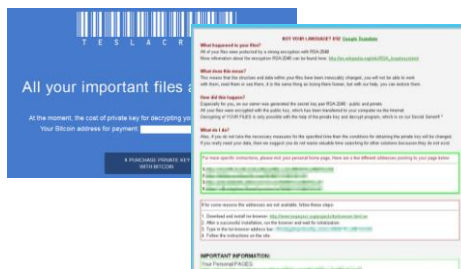
2013 ~ . TorrentLocker Family



2014 ~ . CryptoWall Family



2015 ~ . TeslaCrypt Family



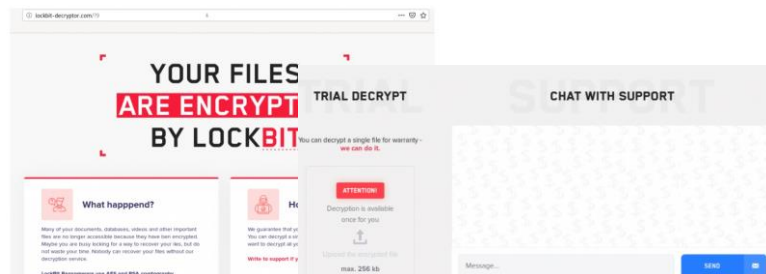
2017 ~ . WanaCrypt Family



2020. Conti

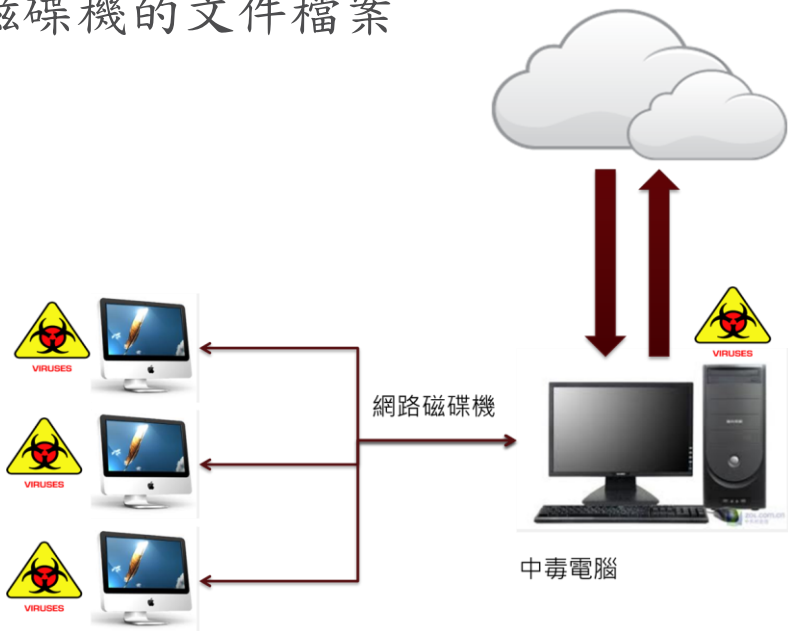


2021 ~ . Lockbit



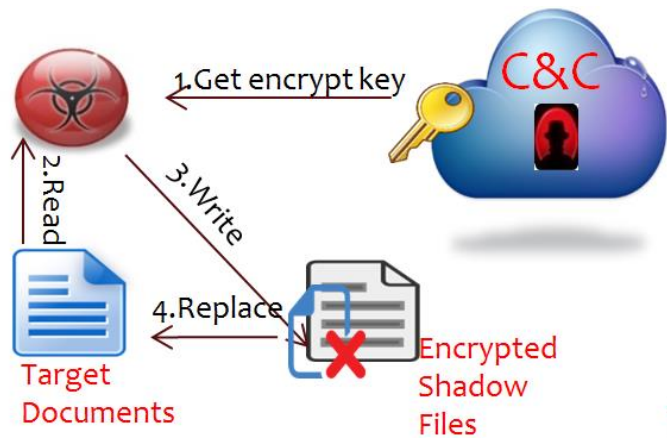
勒索軟體的特性：把你的檔案當作人質 - 加密

- 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



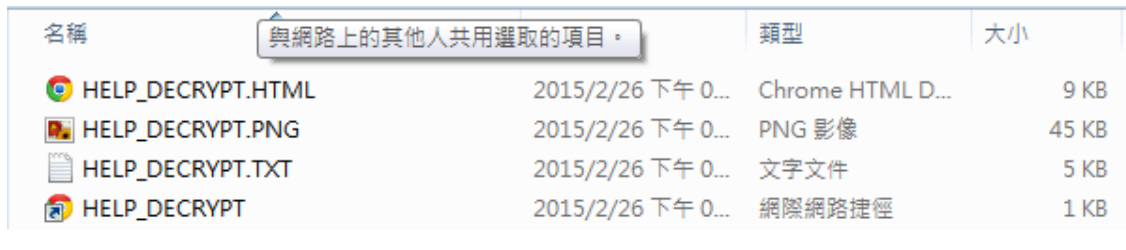
It changes entire file content

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



名稱	日期	類型	大小
13 - Technical Personne...	24/11/2014 11:14 AM	ENCRYPTED File	49 KB
...ng Report.dot.encyr...	24/11/2014 11:14 AM	ENCRYPTED File	51 KB
...dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	27 KB
DECRYPT_INSTRUCTIONS.html	24/11/2014 11:14 AM	HTML Document	7 KB
...tion Report.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	65 KB
Fa...atCert.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	57 KB
...un Report.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	32 KB
h...ed ...ing Report.dot.encyr...	24/11/2014 11:14 AM	ENCRYPTED File	52 KB
Pa... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	610 KB
... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	608 KB
R... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	606 KB
R... Inspection.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	604 KB
V...report.dot.encrypted	24/11/2014 11:14 AM	ENCRYPTED File	38 KB



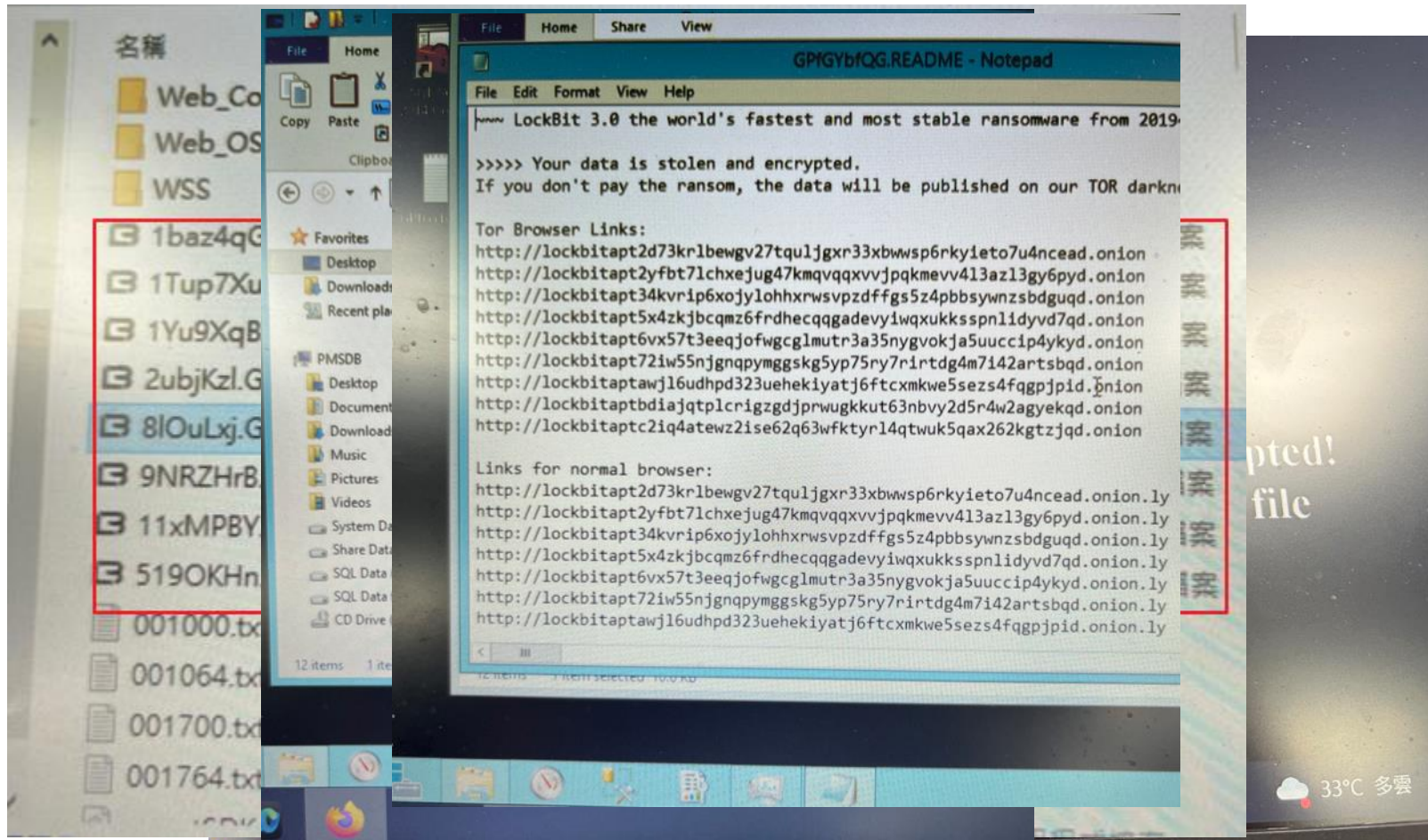
名稱	日期	類型	大小
HELP_DECRYPT.HTML	2015/2/26 下午 0...	Chrome HTML D...	9 KB
HELP_DECRYPT.PNG	2015/2/26 下午 0...	PNG 影像	45 KB
HELP_DECRYPT.TXT	2015/2/26 下午 0...	文字文件	5 KB
HELP_DECRYPT	2015/2/26 下午 0...	網際網路捷徑	1 KB

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



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



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



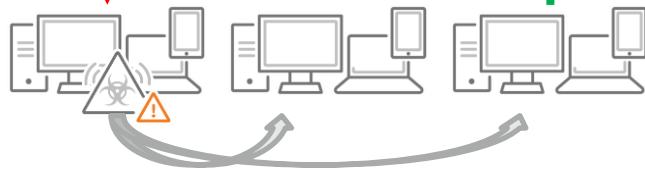
近年常見駭客攻擊手法



建立中繼站連線



透過合法帳號與工
具程式



釣魚電子郵件

水坑攻擊
供應鏈淪陷

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

← → ↻ Chrome | chrome://settings/content/javascript

設定 搜尋設定

- 你與 Google
- 自動填入
- 隱私權和安全性
- 外觀
- 搜尋引擎
- 預設瀏覽器
- 起始畫面
- 進階
- 語言
- 下載
- 無障礙設定
- 系統
- 重設與清理
- 擴充功能
- 關於 Chrome

JavaScript

網站通常會使用 JavaScript，以顯示電玩遊戲或網路表單等互動式功能

預設行為
網站會在你造訪時自動套用這項設定

<> 網站可以使用 JavaScript

禁止網站使用 JavaScript

自訂設定
下列網站採用自訂設定，而非預設設定

不得使用 JavaScript 新增

未新增任何網站

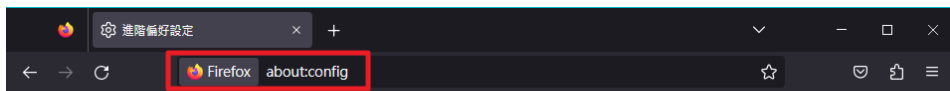
可以使用 JavaScript 新增

未新增任何網站

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」。



調整設定前請務必小心！

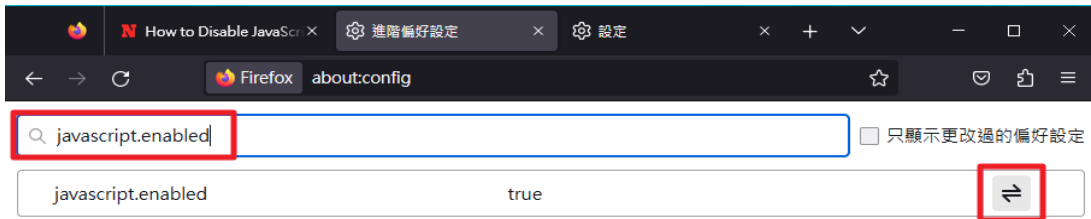
調整進階設定，可能會影響 Firefox 的效能或安全性。

當我嘗試修改偏好設定時警告我

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

The screenshot shows the Firefox browser interface with the 'about:preferences#privacy' page open. The address bar shows the URL and a search box for options. On the left, there is a sidebar with navigation icons for '一般' (General), '首頁' (Home), '搜尋' (Search), '隱私權與安全性' (Privacy & Security), and '同步' (Sync). The main content area is titled '瀏覽器隱私權' (Browser Privacy) and '加強型追蹤保護' (Enhanced Tracking Protection). A shield icon indicates that tracking protection is active, with a note that it blocks many trackers and other scripts. A link to '了解更多' (Learn more) is provided. Below this, there are three sections for tracking protection levels: '標準 (D)' (Standard), '嚴格 (R)' (Strict), and '自訂 (C)' (Custom). The 'Standard' section is selected and highlighted in blue, listing various tracking methods blocked by Firefox. On the right side of the browser, the menu is open, showing options like '同步並儲存資料' (Sync and Save Data), '關新分頁' (New Tab), '關新視窗' (New Window), '關新隱私視窗' (New Private Window), '書籍' (Bookmarks), '歷史' (History), '下載項目' (Downloads), '密碼' (Passwords), '附加元件與佈景主題' (Add-ons and Themes), '列印...' (Print...), '另存新檔...' (Save As...), '在頁面中搜尋...' (Search in Page...), '縮放' (Zoom), '設定' (Settings), '更多工具' (More Tools), '說明' (Help), and '結束' (Quit). The '設定' (Settings) option is highlighted with a red box.

Firefox about:preferences#privacy

搜尋選項

瀏覽器隱私權

加強型追蹤保護

追蹤器會在網路上跟蹤您，收集您的興趣與喜好。Firefox 會封鎖許多追蹤器與其他有書指令碼。 [了解更多](#)

管理例外網站... (X)

- 標準 (D)**
兼顧保護與效能。網站可正常運作。
Firefox 封鎖下列項目：
 - 社交媒體追蹤器
 - 跨網站追蹤 Cookie
 - 隱私視窗中的跨網站 Cookie
 - 隱私視窗中的追蹤內容
 - 加密貨幣採礦程式
 - 數位指紋追蹤程式
- 嚴格 (R)**
保護更強大，但可能會導致某些網站或內容故障。
- 自訂 (C)**
選擇要封鎖哪些追蹤器與指令碼。

同步並儲存資料 登入

關新分頁 Ctrl+T

關新視窗 Ctrl+N

關新隱私視窗 Ctrl+Shift+P

書籍 >

歷史 >

下載項目 Ctrl+J

密碼

附加元件與佈景主題 Ctrl+Shift+A

列印... Ctrl+P

另存新檔... Ctrl+S

在頁面中搜尋... Ctrl+F

縮放 - 100% +

設定

更多工具 >

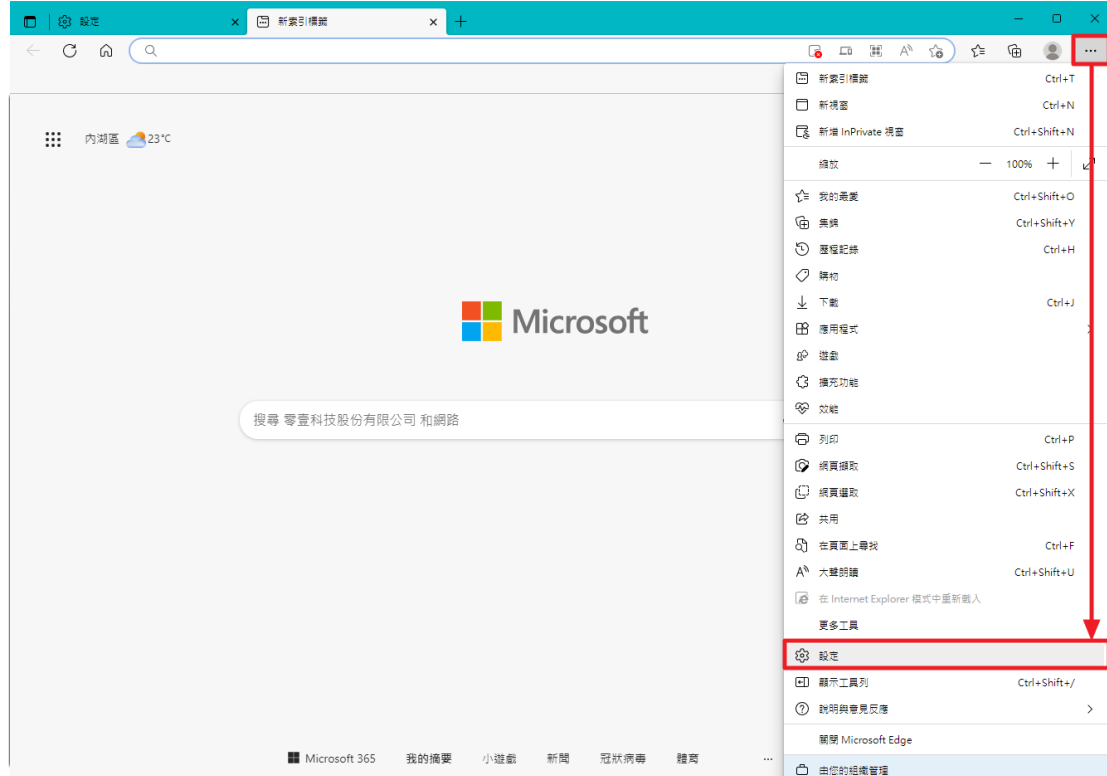
說明 >

結束 Ctrl+Shift+Q

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。

The screenshot displays the Windows Settings application with the Microsoft Edge settings page open. On the left sidebar, the 'Cookie and site permissions' option is highlighted with a red box. The main content area shows a list of permissions, with 'JavaScript' also highlighted by a red box. To the right, the 'JavaScript' permission page is shown, where the '已允許 (建議)' (Allowed) toggle switch is turned off and highlighted with a red box. Below this, there are sections for '封鎖' (Blocked) and '允許' (Allowed), both showing '沒有新增的網站' (No new sites).

設定

搜尋設定

- 個人檔案
- 隱私權、搜尋與服務
- 外觀
- 側邊欄
- 開始、首頁及新索引標籤
- 分享、複製並貼上
- Cookie 和網站權限**
- 預設瀏覽器
- 下載
- 家長監護服務
- 語言
- 印表機
- 系統與效能
- 重設設定
- 手機及其他裝置
- 協助工具
- 關於 Microsoft Edge

僅所有網站上啟用的權限

- 位置
先詢問
- 相機
先詢問
- 麥克風
先詢問
- 動作或光感應器
允許網站使用動態和光感應器
- 通知
先詢問
- JavaScript**
已封鎖
- 影像
全部顯示
- 快顯視窗並重新導向
已封鎖
- 廣告
已封鎖
- 背景同步處理
允許最近關閉的網站完成發送和接收資料
- 自動下載

← 網站權限 / JavaScript

已允許 (建議)

封鎖

沒有新增的網站

允許

沒有新增的網站

收信軟體安全-關閉預覽視窗(Outlook)

The image shows the Outlook interface with the '檢視' (View) ribbon selected. A red box labeled '1' highlights the '檢視' tab. A red box labeled '2' highlights the '讀取窗格' (Read Pane) icon in the ribbon. A dialog box titled '讀取窗格' (Read Pane) is open, with a red box labeled '3' highlighting the '選項(N)...' (Options...) button. A yellow arrow points from the '選項(N)...' button to the '永遠預覽郵件(A)' (Always preview mail) checkbox in the dialog box.

檔案 常用 傳送 / 接收 資料夾 **檢視** 1 明

變更檢視 檢視設定 重設檢視

目前檢視

顯示為交談 顯示為交談

交談設定

日期(D) 寄件者(F) 反向排序 新增欄 展開/折疊

收件者(T) 類別(E)

使用較緊密的間距 資料夾窗格 讀取窗格 2 待辦事項列

右(R) 下(B) 關閉(O) 3 選項(N)...

將您最愛的資料夾拖曳到這裡

全部 未讀取

我們找不到任何項目可在

收件匣 238

草稿

讀取窗格

讀取窗格選項

於讀取窗格中檢視過即標示為已讀取(M)

在項目標示為已讀取前等候(W) 5 秒

變更選取時，將項目標示為已讀取(R)

使用空格鍵單鍵閱讀(S)

開啟直向的自動全螢幕讀取(T)

永遠預覽郵件(A)

確定 取消

收信軟體安全-關閉自動圖片下載(Outlook)

Outlook 選項

一般
郵件
行事曆
群組
人員
工作
搜尋
語言
協助工具
進階

自訂功能區
快速存取工具列
增益集

信任中心 1

協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。

安全性和其他

造訪 Office.com 以瞭解更多關於保護您的隱私權和安全性的資訊。

[Microsoft 信任中心](#)

Microsoft Outlook 信任中心

信任中心包含安全性和隱私權設定。這些設定將協助您保持電腦的安全性。我們建議您不要變更這些設定 2 **信任中心設定(D)...**

信任中心

您可以控制 Outlook 是否要在開啟 HTML 電子郵件訊息時自動下載及顯示圖片。

封鎖電子郵件訊息中的圖片可協助保護您的隱私。HTML 電子郵件中的圖片可以要求 Outlook 從伺服器下載圖片。利用此種方式與外部伺服器通訊會讓寄件者確認您的電子郵件地址是有效的，您可能因此成為垃圾郵件的目標。

- 不自動下載標準 HTML 電子郵件訊息或 RSS 項目中的圖片(D)
- 允許來自或傳送到垃圾郵件篩選使用之 [安全寄件者清單] 和 [安全收件者清單] 中定義的寄件者或收件者的電子郵件訊息中下載(S)
- 允許自這個安全性區域的網站下載(P): 信任的區域
- 允許 RSS 項目中的下載(R)
- 允許 SharePoint 討論區中的下載(B)
- 當編輯、轉寄或回覆電子郵件時，在下載內容前先警告我(W)
- 不下載已加密或已簽章之 HTML 電子郵件訊息中的圖片

自動下載 3

巨集設定
以程式設計方式存取

受信任的發行者
隱私權選項
表單型登入
電子郵件安全性
附件處理

確定 取消

確定 取消

收信軟體安全-以純文字閱讀(Outlook)

Outlook 選項

? X

一般
郵件
行事曆
群組
人員
工作
搜尋
語言
協助工具
進階

自訂功能區
快速存取工具列
增益集

信任中心 **1**

受信任的發行者
隱私選項
表單型登入
電子郵件安全性 **3**
附件處理
自動下載
巨集設定
以程式設計方式存取

協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。

安全性和其他

造訪 Office.com 以瞭解更多關於保護您的隱私權和安全性的資訊。

[Microsoft 信任中心](#)

Microsoft Outlook 信任中心

信任中心包含安全性和隱私權設定。這些設定將協助您保持電腦的安全性。我們建議您不要變更這些設定 **2**

信任中心設定(I)...

信任中心

預設設定(E): [] 設定(S)...

數位識別碼(憑證)

數位識別碼或憑證是在電子交易中供您證明身分的文件。

發佈到 GAL(P)... 匯入/匯出(I)...

以純文字讀取

以純文字讀取所有標準郵件(A)

以純文字讀取所有數位簽章的郵件(M)

資料夾的指令碼

共用資料夾允許指令碼(L)

公用資料夾允許指令碼(E)

確定 取消

確定

取消

收信軟體安全-關閉附件預覽(Outlook)

Outlook 選項

? X

一般
郵件
行事曆
群組
人員
工作
搜尋
語言
協助工具
進階

自訂功能區
快速存取工具列
增益集

信任中心 **2**

受信任的發行者
隱私選項
表單型登入
電子郵件安全性
附件處理 **3**
自動下載
巨集設定
以程式設計方式存取

協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。

安全性和其他

造訪 Office.com 以瞭解更多關於保護您的隱私權和安全性的資訊。

[Microsoft 信任中心](#)

Microsoft Outlook 信任中心

信任中心包含安全性和隱私權設定。這些設定將協助您保持電腦的安全性。我們建議您不要變更這些設定 **1** [信任中心設定\(D\)...](#)

信任中心 ? X

附件安全性模式

安全性模式: 預設

回覆變更

新增內容至附件以啟用回覆變更(A)

附件與文件預覽

[關閉附件預覽\(D\)](#)

[附件與文件預覽器\(P\)](#)

確定 取消

確定


取消

收信軟體安全-不要自動回覆讀信回條 (Outlook)

Outlook 選項

一般
郵件
行事曆
群組
人員
工作
搜尋
語言
協助工具
進階
自訂功能區
快速存取工具列
增益集
信任中心

追蹤

 送達和讀信回條可協助確認收件者已成功收到郵件。並非所有電子郵件伺服器 and 應用程式都支援傳送回條的功能。
對於所有送出的郵件、邀請:

- 確認郵件已送達收件者電子郵件伺服器的送達回條(X)
- 確認收件者已檢視郵件的讀信回條(B)

對於任何含有索取讀信回條的已收到郵件:

- 永遠傳送讀信回條(A)
- 不要傳送讀信回條(N)
- 每次詢問是否要傳送讀信回條(M)

- 自動處理會議邀請及會議邀請和投票的回覆(O)
- 自動更新含回條資訊的原始信件(E)
- 更新追蹤資訊，並刪除不含註解的回覆(U)
- 更新追蹤資訊後，將回條移到(P):

郵件格式

- 使用階層式樣式表 (CSS) 作為郵件外觀(L)
- 移除顯示郵件時不需要的格式資訊，以減少郵件大小(F)
- 傳送純文字郵件時，以 UUENCODE 格式編碼附件(U)

達下列字數時自動換列(C):

- 移除純文字郵件中多餘的分行符號(X)

傳送 RTF 格式的郵件給網際網路收件者時(W):

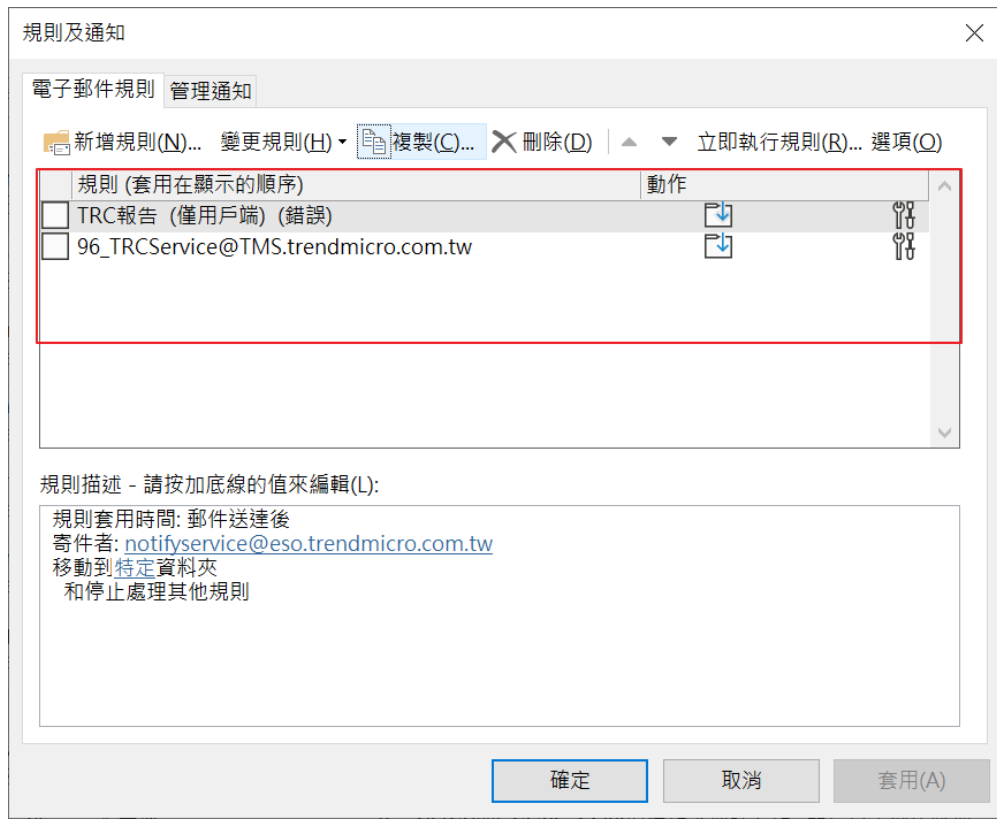
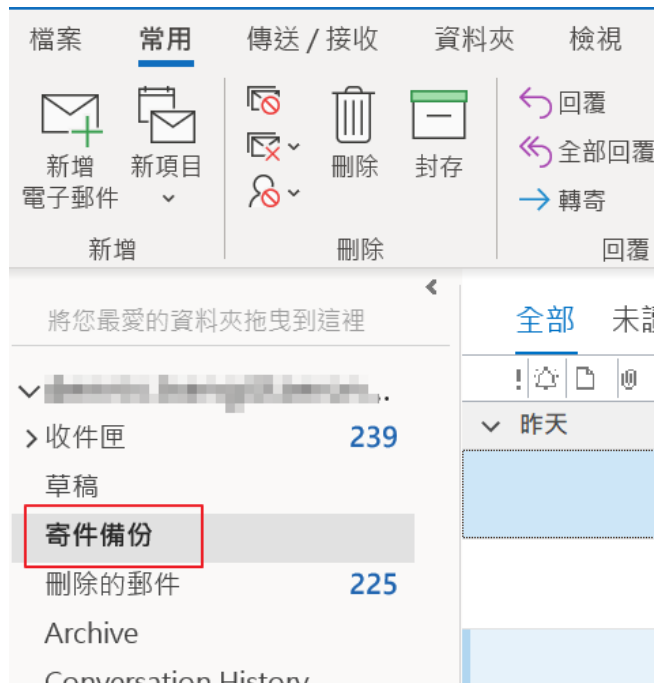
其他

- 將內容貼入郵件時顯示 [貼上選項] 按鈕(P)
- 閱讀郵件時，在郵件標題中顯示 [下一封] 和 [上一封] 連結(H)
- 使用鍵盤變更郵件時，不自動展開交談(I)

確定

取消

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

勒索軟體防護專區 遠距辦公資安專區 回首頁 網站導覽 訂閱電子報 English

新聞公告 News 資安服務 Services 資安宣導 Advocacy 相關網站 Links 關於我們 About us 

首頁 / 新聞公告 / 資安新聞

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

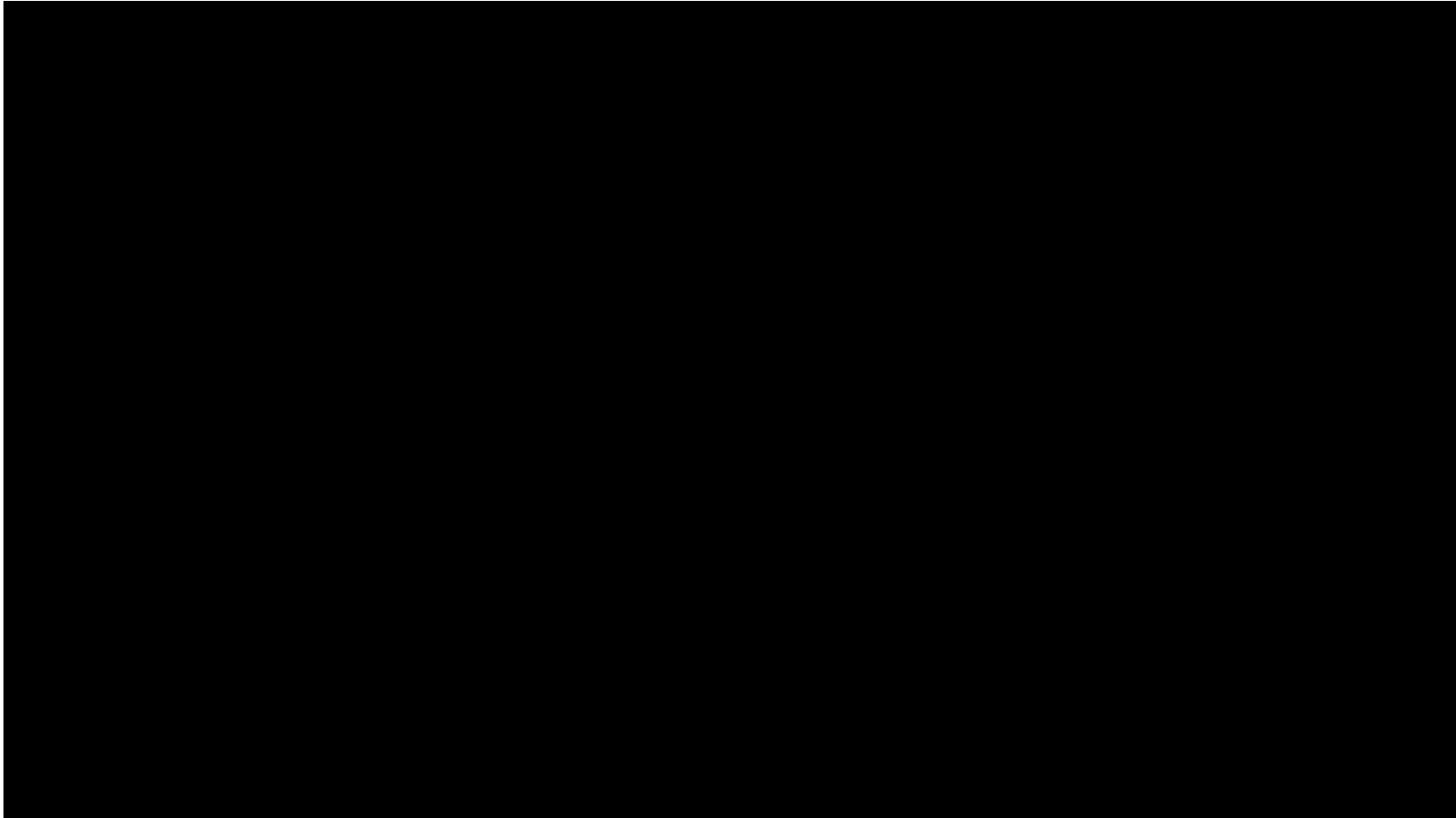
◎發布日期：2022-03-07 字型大小： 小 中 大 

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，駭業者將能在 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

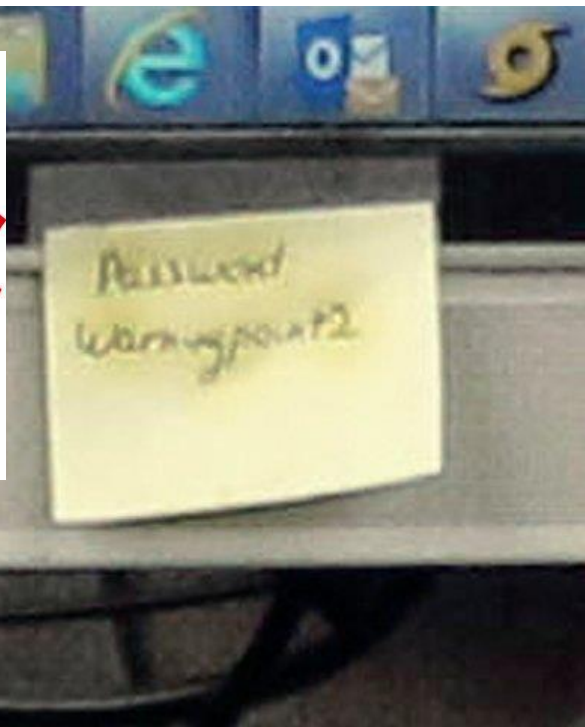
進階例1：123QAZwsx!!@@##Go0gl1

進階例2：123QAZwsx!!@@##F@c1bo0k

密碼不安全行為



密碼不安全行為

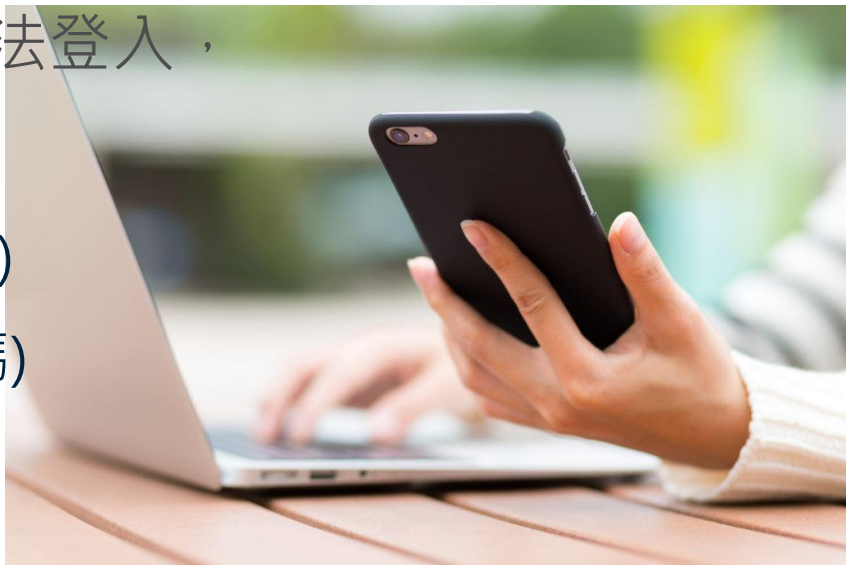


Two-Factor Authentication (2FA)

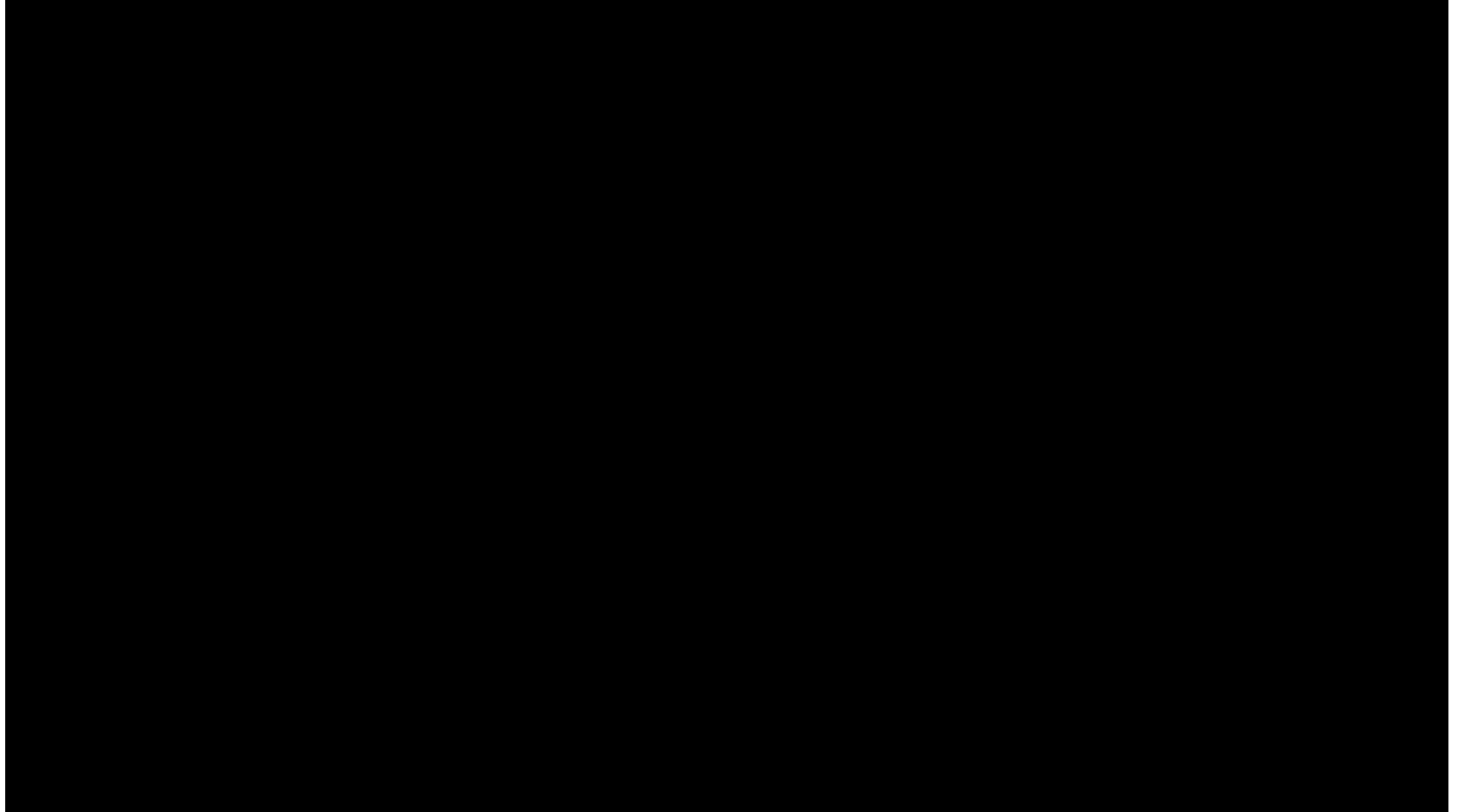
雙重驗證可提供多一層保障，使罪犯較難進行未授權的存取動作

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

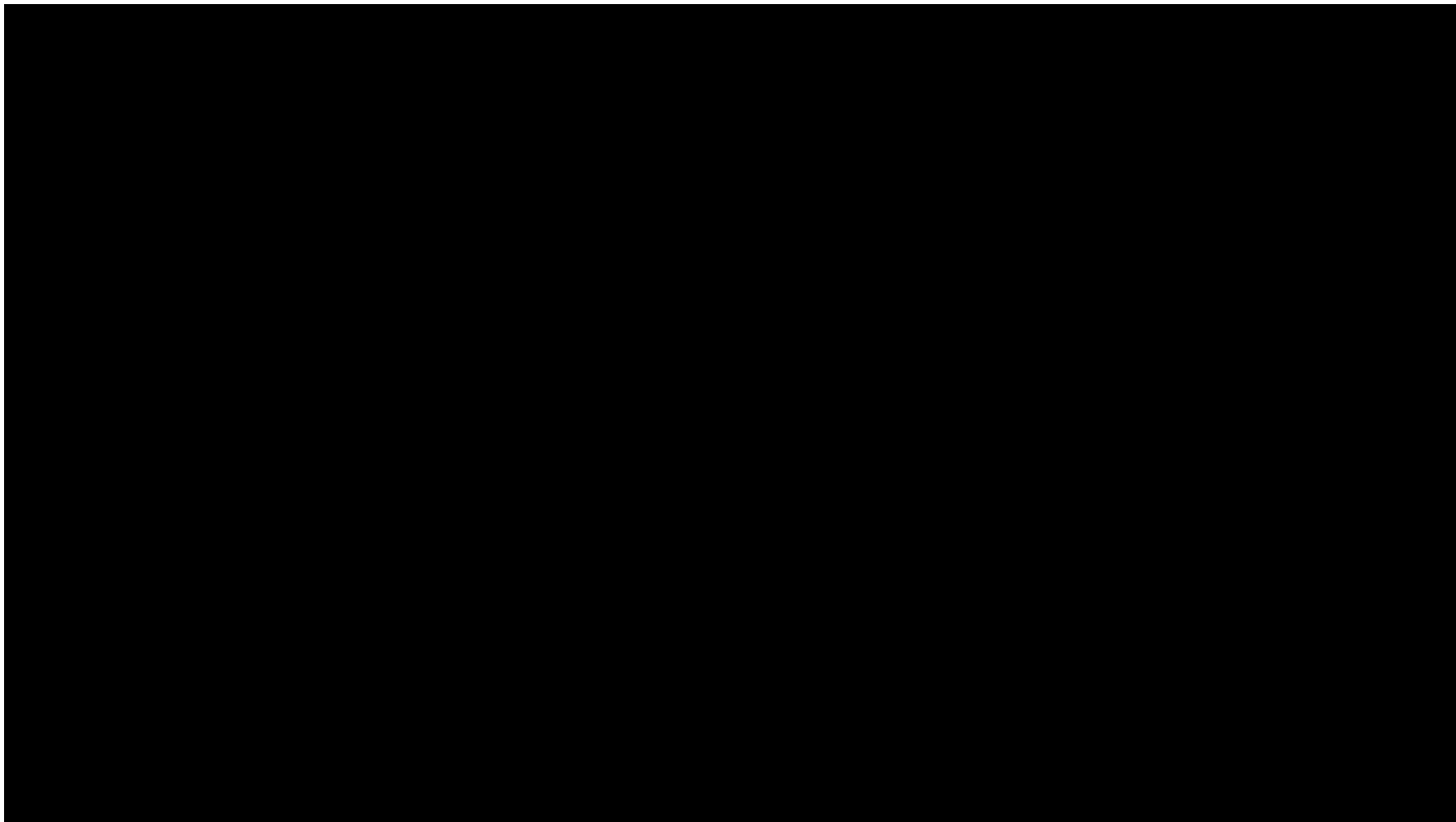


資料隱私一直以來都很重要。

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 address}.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

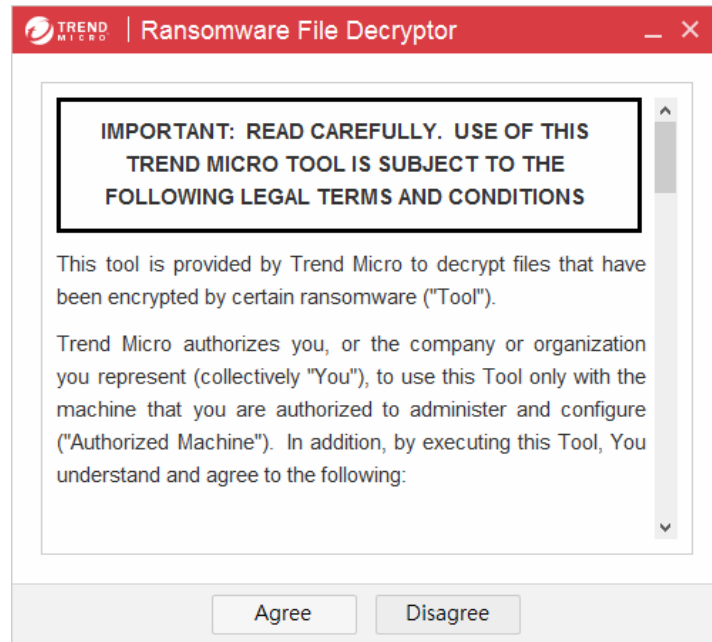
工具下載：

- 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>

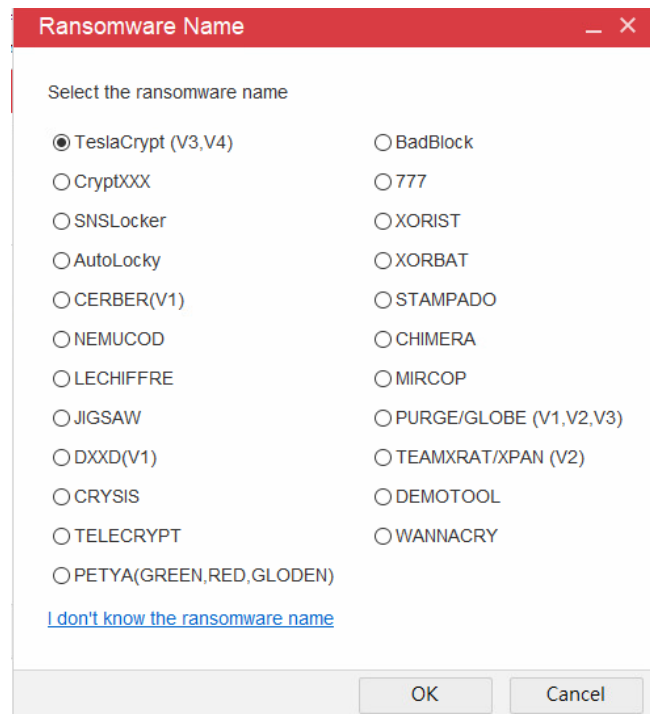
勒索軟體-解密工具

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



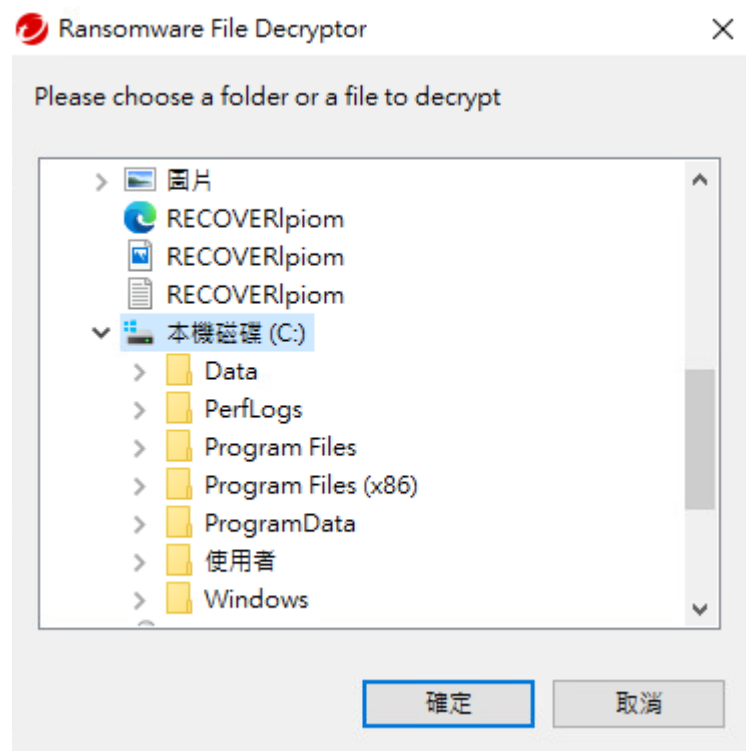
勒索軟體-解密工具

- 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。



The screenshot shows the 'Ransomware File Decryptor' application window. The title bar includes the Trend Micro logo and the text 'Ransomware File Decryptor'. Below the title bar is a header section with a blue padlock icon and the text 'Anti-Ransomware' and 'Trend Micro experts help you decrypt your encrypted files'. The main content area displays 'Scan Completed' with a duration of '00:00:00'. A yellow box highlights the statistics: 'Infected files: 5' and 'Decrypted files: 5', with a blue link 'See decrypted' next to the latter. A 'Done' button is visible to the right. At the bottom, there is a red promotional banner for 'Trend Micro Ransom Buster' with the slogan 'An ounce of prevention is worth a pound of cure!' and a 'FREE' badge. The footer contains links for 'Trend Micro Support Website' and 'Feedback'.

TREND MICRO | Ransomware File Decryptor

Anti-Ransomware
Trend Micro experts help you decrypt your encrypted files

Scan Completed
Duration: 00:00:00

Infected files: 5
Decrypted files: 5 [See decrypted](#)

Done

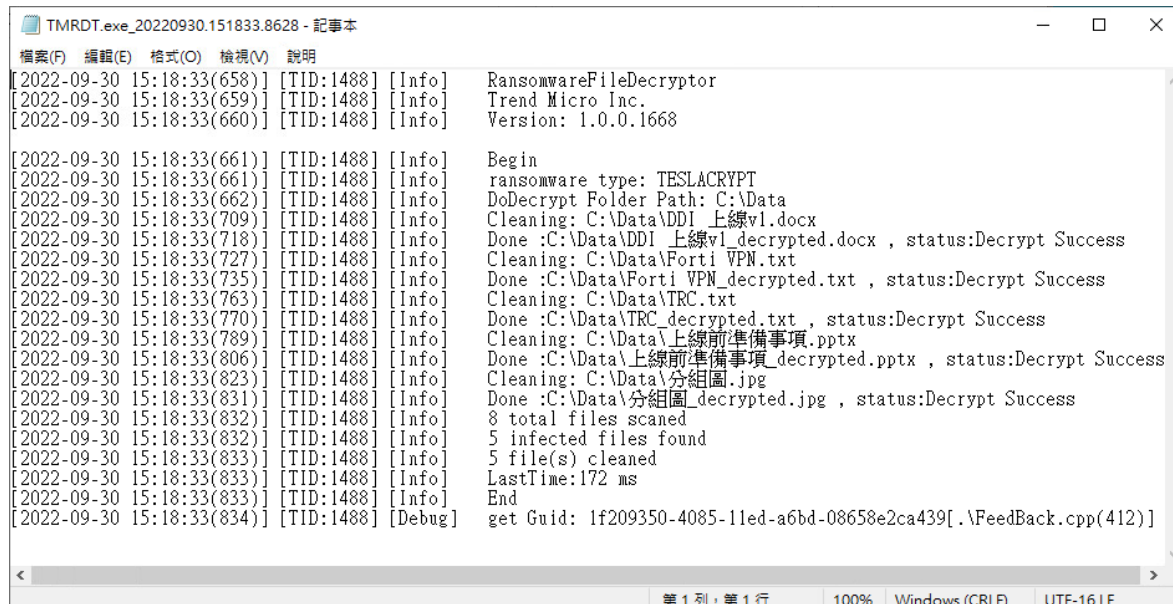
An ounce of prevention is worth a pound of cure!
Trend Micro Ransom Buster
FREE

[Trend Micro Support Website](#) [Feedback](#) ⓘ

勒索軟體-解密工具

- 工具記錄檔

%User%\AppData\Local\Temp\TMRDTSelfExtract\LOG



```
TMRDT.exe_20220930.151833.8628 - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
[2022-09-30 15:18:33(658)] [TID:1488] [Info] RansomwareFileDecryptor
[2022-09-30 15:18:33(659)] [TID:1488] [Info] Trend Micro Inc.
[2022-09-30 15:18:33(660)] [TID:1488] [Info] Version: 1.0.0.1668

[2022-09-30 15:18:33(661)] [TID:1488] [Info] Begin
[2022-09-30 15:18:33(661)] [TID:1488] [Info] ransomware type: TESLACRYPT
[2022-09-30 15:18:33(662)] [TID:1488] [Info] DoDecrypt Folder Path: C:\Data
[2022-09-30 15:18:33(709)] [TID:1488] [Info] Cleaning: C:\Data\DDI 上線v1.docx
[2022-09-30 15:18:33(718)] [TID:1488] [Info] Done :C:\Data\DDI 上線v1_decrypted.docx , status:Decrypt Success
[2022-09-30 15:18:33(727)] [TID:1488] [Info] Cleaning: C:\Data\Forti VPN.txt
[2022-09-30 15:18:33(735)] [TID:1488] [Info] Done :C:\Data\Forti VPN_decrypted.txt , status:Decrypt Success
[2022-09-30 15:18:33(763)] [TID:1488] [Info] Cleaning: C:\Data\TRC.txt
[2022-09-30 15:18:33(770)] [TID:1488] [Info] Done :C:\Data\TRC_decrypted.txt , status:Decrypt Success
[2022-09-30 15:18:33(789)] [TID:1488] [Info] Cleaning: C:\Data\上線前準備事項.pptx
[2022-09-30 15:18:33(806)] [TID:1488] [Info] Done :C:\Data\上線前準備事項_decrypted.pptx , status:Decrypt Success
[2022-09-30 15:18:33(823)] [TID:1488] [Info] Cleaning: C:\Data\分組圖.jpg
[2022-09-30 15:18:33(831)] [TID:1488] [Info] Done :C:\Data\分組圖_decrypted.jpg , status:Decrypt Success
[2022-09-30 15:18:33(832)] [TID:1488] [Info] 8 total files scanned
[2022-09-30 15:18:33(832)] [TID:1488] [Info] 5 infected files found
[2022-09-30 15:18:33(833)] [TID:1488] [Info] 5 file(s) cleaned
[2022-09-30 15:18:33(833)] [TID:1488] [Info] LastTime:172 ms
[2022-09-30 15:18:33(833)] [TID:1488] [Info] End
[2022-09-30 15:18:33(834)] [TID:1488] [Debug] get Guid: 1f209350-4085-11ed-a6bd-08658e2ca439[.\Feedback.cpp(412)]

第 1 列, 第 1 行 100% Windows (CRLF) UTF-16 LE
```

解密工具操作影片

File Edit View VM Tabs Help

Dennis_Win10_Client_10_... x

RECOVERpiom.html x +

RECOVERpiom.html

C:/ProgramData/Microsoft/Windows/Start%20Menu/Programs/StartUp/RECOVERpiom.html

相片 - RECOVERpiom.png

查看所有相片 + 新增蓋章

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_\(cryptosystem\)](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://uhfmsad7bhfykqfvevmxergwrth.himfinn.com/64DFEE8488E38D85>
- <http://94dhhb3j4blaeyfgl7q45glbaer.giponfeste.at/64DFEE8488E38D85>
- <http://h5nuwe8kub134jngkasdhasfn.cortolbugan.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. Enter the following link in the address bar: k7hr1gbr3m4n7u.onion/64DFEE8488E38D85

!!! IMPORTANT INFORMATION:

Your personal homepage:
<http://uhfmsad7bhfykqfvevmxergwrth.himfinn.com/64DFEE8488E38D85>
<https://94dhhb3j4blaeyfgl7q45glbaer.giponfeste.at/64DFEE8488E38D85>
<http://h5nuwe8kub134jngkasdhasfn.cortolbugan.com/64DFEE8488E38D85>

Your personal page for Browser: k7hr1gbr3m4n7u.onion/64DFEE8488E38D85

Your personal identification ID: 64DFEE8488E38D85

RECOVERpiom - 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/wiki/RSA_\(cryptosystem\)](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.

第 1 列 · 第 1 行 100% Windows (CRLF) UTF-8

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



別再用Facebook帳號登入 APP！
用這招解除一鍵登入的個資外洩風險

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



點選「設定」進行編輯



點選「應用程式和網站」，顯示



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 [redacted] 5



備援電子郵件

 請驗證 k [redacted] @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
Ac [redacted] lax
Mz [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

Ads by Google

新竹寶山美地-晴山農園 www.ezfarm.com.tw

距交流道、市區、便利商店只要5分鐘 下班後最舒服自在的溫馨小屋



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，查一查自己有無其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

新聞 政治 社會 國際 兩岸 地方 財經 科技 運動 娛樂 生活

詐騙手法鎖定車主 交通罰單簡訊恐遭騙

新聞網

分享 2



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，完成申訴程序時還可查詢申訴案件的處理進度。

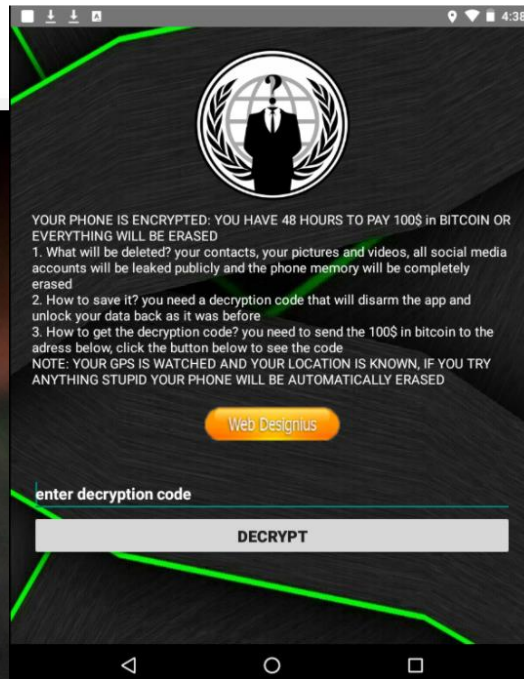
除了簡訊詐騙要當心，對於電話詐騙也不能掉以輕心，像是台北市一位74歲郭姓老婦人，接獲電話表示身分遭盜用，若要排除嫌疑必須提領戶頭內所有現金交付檢察官保管，以利案件偵辦，甚

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 / 記者黃馨祥



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

Tweet 0 +1 0 分享 2 讚 2 Pin It in Share

讚 2 +1 0 推文 0 Share Submit

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!勒索集團威發瀏覽色情網站 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)



будет автоматически разблокирован, если данные будут удалены с серверов КИБ, в уголовное дело прекращено.

23:59:37

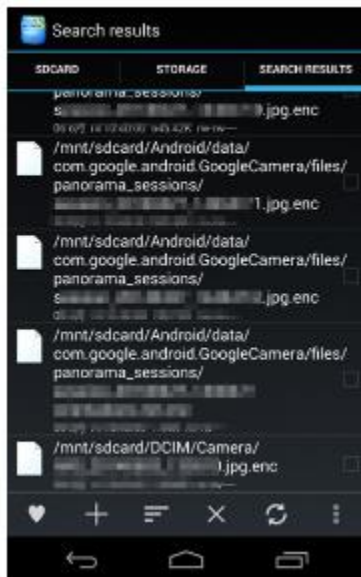
При попытках выключения или перезапуска устройства, СЧЕТЧИК ВРЕМЕНИ будет автоматически уменьшаться на час, при полностью выключенном устройстве, СЧЕТЧИК ВРЕМЕНИ продолжает работать. Если оплата штрафа не поступит в течение 24 ч сумма штрафа удваивается. Если оплата штрафа не поступит в течение 48 ч - всем контактам Вашего устройства, будет отправлено смс уведомление от имени КИБ Российской Федерации (Со сдержанием вашего Звонка), о том что интерфейс Вашего устройства был ЗАБЛОКИРОВАН ЗА НЕОДНОКРАТНОЕ ПОСЕЩЕНИЕ САЙТОВ СОДЕРЖАЩИЕ ВИДЕО СО СЦЕНАМИ ДЕТСКОЙ ПОРНОГРАФИИ, а также на основании ст. 242 УК РФ, ст. 41 КАС РФ и ст. 31 УКП РФ, по месту жительства, будет отправлен наряд для сбора вещественных доказательств, изъятия заблокированного устройства и вашего задержания для дачи пояснения.

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 Play、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



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蹤](#)

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



Line免費貼圖詐騙



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

HTM 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

Version: What's This? What's This?

假冒信件

MyCard安全性通知

收件匣 x

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.....@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)

收件者: 零壹科技全體同仁; 羽祥團隊; 兩字科技

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券~
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,日常工作與資安風險的拉鋸,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: 711禮券100元,符合參加標準,人人有獎,禮券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
 當天直播連結底家,請於會議前2分鐘點我連線

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

<https://forms.office.com/Pages/ResponsePage.aspx?id=XnJ79wkgHkyJqVJbeNSKuZeLeDm4BupCpx0wllMPcjdURDNOSUNVWUIHOFI0R09LWldGVDAxSVJMOC4u>

檢查連結

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

Best Regards,

<https://z1meeting.webex.com/z1meeting/j.php?MTID=m17a08c915b5a3682d37869b2ee6f9c37>

假冒網站



://facebook.com/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



假冒網站



假冒網站

官方正確網址應為.gov.tw



▲ 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



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!



免運費/貨到付款/送限定保護殼/正品保證 假一賠十?!

好市多一頁式詐騙廣告 騙下單送假貨!



小心收到劣質品

Mascotnow.online-2
贊助

為慶賀好市多 #創造840億年營收
總裁決定每日推出20個AirPods 3代“聯手”AirPods Pro 雙拳出擊!
每人限購一次!
>>>https://vip.mascotnow.online/twcostco

COSTCO WHOLESALE

總有一個你想要的!

AirPods 3代 (無線藍牙)
AirPods Pro (無線藍牙)

詐騙警訊

FAT TIGER

VIPMASCOTNOW ONLINE
【贈送虎年保護殼】新年特惠 每人限購一次! 瞭解詳情
正品保證,假一賠十

假冒網站

your.message-unread.com/tw/px_mart/clean-back-doman-hk-php.php?pkkey=165952af33cd248519&domain=push.apush-link.click&uclid=7sqd37a2&uclidhash=7sqd37a2-7sqd37a2-b4u3-0-2ta8-sihe-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



假冒 QR Code

QR Code 真假？

2022國旅補助懶人包

申請資格、加碼金額、民宿清單



請留意! 請留意! 透過此平台預訂"不適用"旅遊補助
請掃描下方QR CODE至官網預訂

國旅補助適用專區

預訂請掃描
QR Code!



— 名稱有誤，國旅補助規定，係政府公告為主 —

旅遊補助 懶人包

政府補助 就是要你出去玩



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



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

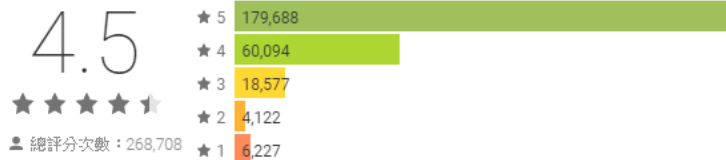
如何下載安全的軟體

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

評論

撰寫評論



其他資訊

發佈日期	大小	安裝次數
2016年1月22日	17M	10,000,000 - 50,000,000

目前版本	Android 最低版本需求	內容分級
2.0.1028	2.3 以上	3 歲以上
		瞭解詳情

權限	檢舉	提供者
查看詳細資訊	檢舉不當內容	Trend Micro

開發人員
造訪網站
將電子郵件寄到 freemobile@trendmicro.com
[隱私權政策](#)
225 John Carpenter Freeway, Suite 1500 Irving,
Texas 75062 U.S.A.

郵件安全性

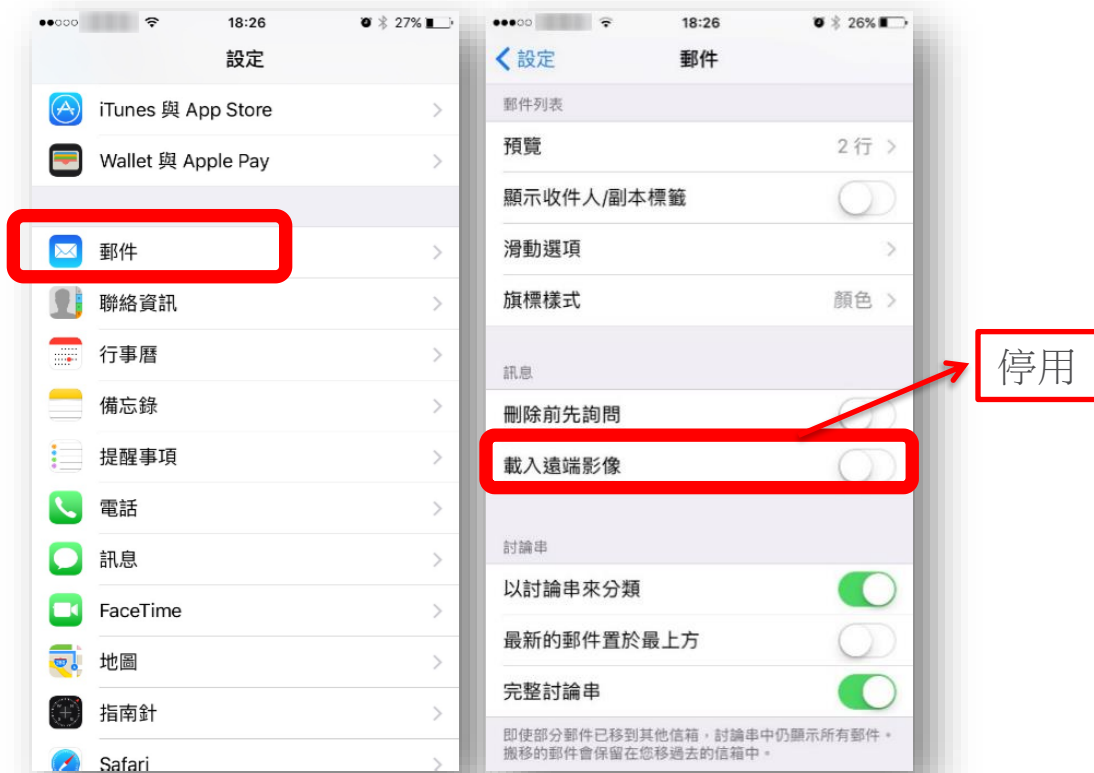
The screenshot shows an email client window with several annotations:

- A yellow box highlights the sender information area, containing the labels "寄件人名稱" (Sender Name) and "寄件人email" (Sender Email).
- A yellow arrow points from the text "詐騙集團仿冒完全一樣的寄件人名稱" (Scam groups impersonate completely identical sender names) to the "寄件人名稱" label.
- A yellow arrow points from the text "收件人難以察覺來自於不同的寄件人" (Recipients find it difficult to notice emails from different senders) to the "寄件人email" label.
- An orange arrow points from the text "點選開啟寄件人電子郵件" (Click to open sender's email) to the "寄件人email" label.
- Below the orange arrow, red text says "確認與原廠商email相同" (Confirm it is the same as the original manufacturer's email).

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

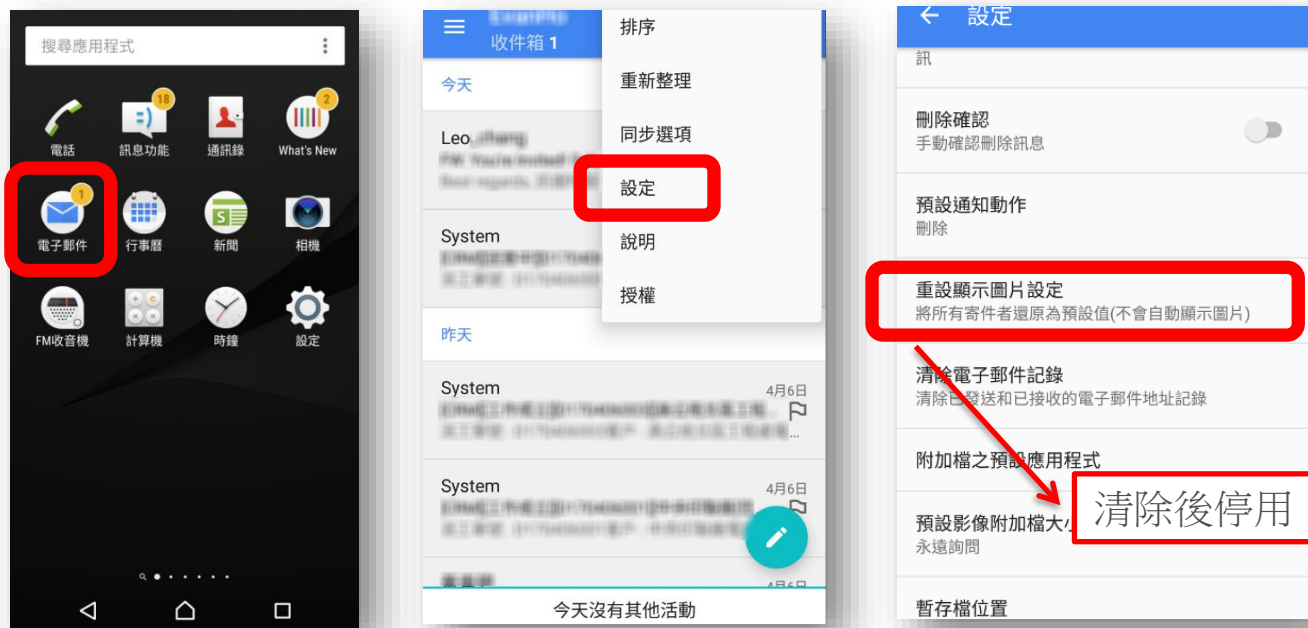
內政部 刑事警察局

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

The image shows a screenshot of the Facebook account security settings page. The page title is "帳號安全和登入" (Account Security and Login). The left sidebar contains navigation options: "建立粉絲專頁", "建立社團", "新社團", "建立廣告", "在 Facebook", "活動紀錄", "動態消息", "設定", and "登出". The "帳號安全和登入" option is highlighted with a red box. The main content area shows "你登入時所在的位置" (Locations where you've logged in) with two entries: "Windows 電腦 · Taoyüan, Taiwan" (Firefox · 目前在線上) and "Samsung Galaxy Note 5 · Taoyüan, Taiwan" (Messenger · 17小時前). A "查看更多" (View more) link is at the bottom. A red box highlights a three-dot menu icon in the top right corner of the list, which has opened a small menu with "不是你嗎?" (Not you?) and "登出" (Log out) options. The "登出" option is also highlighted with a red box.

建立粉絲專頁

建立社團

新社團

建立廣告

在 Facebook

活動紀錄

動態消息

設定

登出

搜尋

首頁 尋找朋友

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

软件授权: 破解版

更新时间: 2022-03-31

应用平台: Win7,Win8,WinXP

软件语言: 简体中文

软件类别: 网络共享

官方网站: www.nokia88.com

软件等级: ★★★★★



11.1%



88.9%

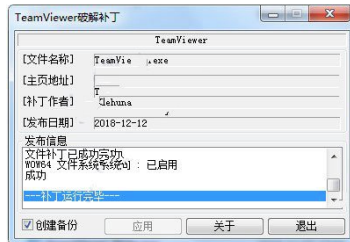


网盘下载

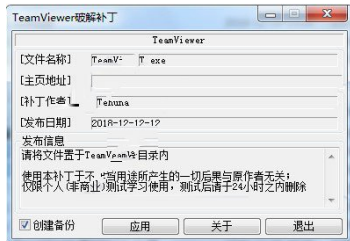
需跳转网盘下载

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



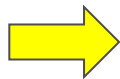
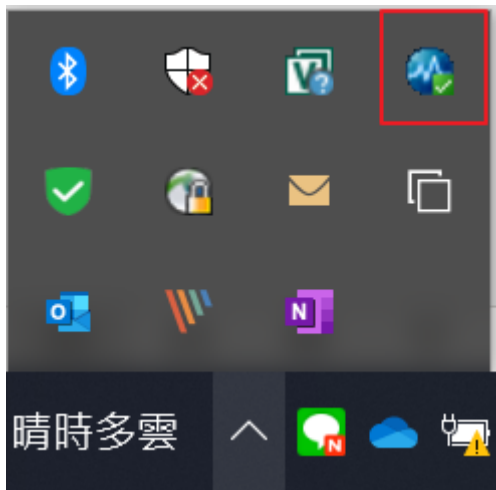
- 3、然后点击【应用】按钮，等待软件破解完成，提示成功，如下图所示：



ApexOne 用戶端介面

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

TREND MICRO | Apex One Security Agent

 安全防護已啟動
您的電腦已受保護，且軟體為最新版本

病毒/惡意程式 0
從 2020/10/27 (週二) 13:52 開始

間諜程式/可能的資安威脅程式 0
從 2020/10/27 (週二) 13:52 開始

預約掃描 已關閉
預約掃描已關閉

本機雲端病毒碼 16.329.00
上次更新時間：無

 掃描

 更新

手動掃描

選取要掃描的資料夾



 掃描

 取消

ApexOne用戶端介面

TREND MICRO | Apex One Security Agent ? _ X

 安全防護已啟動
您的電腦已受保護，且軟體為最新版本

病毒/惡意程式	0
從 2020/10/27 (週二) 13:52 開始	
間諜程式/可能的資安威脅程式	0
從 2020/10/27 (週二) 13:52 開始	
預約掃瞄	已關閉
預約掃瞄已關閉	
本機雲端病毒碼	16,329.00
上次更新時間：無	

 掃瞄

 更新

更新 ? _ X

正在連線至伺服器...

正在連線至伺服器...

已用時間：0:00:05

停止

ApexOne用戶端介面

TREND MICRO | Apex One Security Agent

 安全防護已啟動
您的電腦已受保護，且軟體為最新版本

病毒/惡意程式 1
從 2020/11/5 (週四) 13:18 開始

間諜程式/可能的資安威脅程式 0
從 2020/11/5 (週四) 13:18 開始

預約掃瞄 已啟動
在每週週五的 12:30

本機雲端病毒碼 16.361.00
上次更新時間：2020/11/20

 掃瞄

 更新



設定

系統

記錄檔維護

您想要保留記錄檔資料多長時間？(1 到 60 天)

病毒/惡意程式資料： 15 天

間諜程式/可能的資安威脅程式資料： 15 天

防火牆資料： 7 天

網頁信譽評等資料： 15 天

行為監控資料： 15 天

周邊設備存取控管資料： 15 天

可疑連線資料： 15 天

可疑檔案資料： 15 天

確定 取消 套用

ApexOne用戶端介面



TREND MICRO | Apex One Security Agent

 安全防護已啟動
您的電腦已受保護，且軟體為最新版本

病毒/惡意程式 0
從 2022/9/15 (週四) 08:01 開始


間諜程式/可能的資安威脅程式 0
從 2022/9/15 (週四) 08:01 開始

預約掃瞄 已啟動
在每週週五的 12:00

本機雲端病毒碼 17,841.00
上次更新時間：2022/9/30

掃瞄
更新

🔒 📊 ⚙️ 🌱



記錄檔

範圍： 所有

類型： 病毒/惡意程式 所有結果 (0)

未找到任何記錄

(記錄檔資料只保留 15 天)

關閉

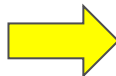
ApexOne用戶端介面

- [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



元件版本

上次更新時間： 2022/9/30
用戶端版本： 14.0.11734
用戶端 GUID： 66e9156e-53ef-46da-82dd-01d8a3c93b32
用戶端通訊埠： 21112
伺服器名稱/通訊埠： lbhbwy.manage.trendmicro.com:443
檔案信譽評等服務： <https://osce14.icrc.trendmicro.com/tmcss> (可用)
網頁信譽評等： <https://osce14-0-tc.url.trendmicro.com> (可用)
可疑物件清單： 2022/3/17 (週四) 21:42

元件	版本	上次更新時間
病毒掃描引擎 (64 位元)	22.510.1003	2022/3/16
本機雲端病毒碼	17.841.00	2022/9/30
IntelliTrap 例外病毒碼	1.961.00	2022/9/28
IntelliTrap 病毒碼	0.253.00	2022/2/7
記憶體檢測病毒碼	1.584.00	2022/2/7
關聯式智慧型查詢處理程式 (64 ...	1.2.1001	
進階安全威脅關聯病毒碼	1.249.00	2022/9/27
Machine Learning 本機檔案模式	2.185.00	2022/9/29
進階安全威脅遙測特徵碼	0.123.00	

關閉

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!
