

# 個人資料保護 與資訊安全

楊玉文

0912811708

alexmysir@gmail.com



# 授課大綱

個資  
保護

個資  
防範

個資  
外洩

資訊  
安全





# 免費網路藏危機。個資恐外洩

百億黑色產業鏈

駭客設釣魚網站 偽免費網路

竊取用戶個資

不肖業者收取個資

發簡訊.e-mail 網路轉手再銷個資



8月製造業PMI



DOW  
16229.32  
▲ 170.97

22:44

埋伏逮嫌 撞警毒品通緝犯 逃亡12天理髮時被逮

# 2017

## 攻擊排名



**Malwarebytes**

•流氓軟體  
Hijacker

1

•廣告軟體  
Adware

2

•風險軟體  
Riskware

3

•木馬程式  
Backdoor

4

•勒索軟體  
Ransomware

5

# 個資重要性

長相、姓名...

經濟、電話...





# 資料在哪裡?



硬碟



雲端硬碟



單位主機



隨身碟



行動設備

# 個資保護的目的



避免人格權  
受侵害

促進個人資料  
合理利用

# 個資保護

不限於經電腦處理

任何自然人、團體與行政法人

於中華民國領域外對中華民國人民蒐集、處理或利用個人資料



# 個人資料保護法

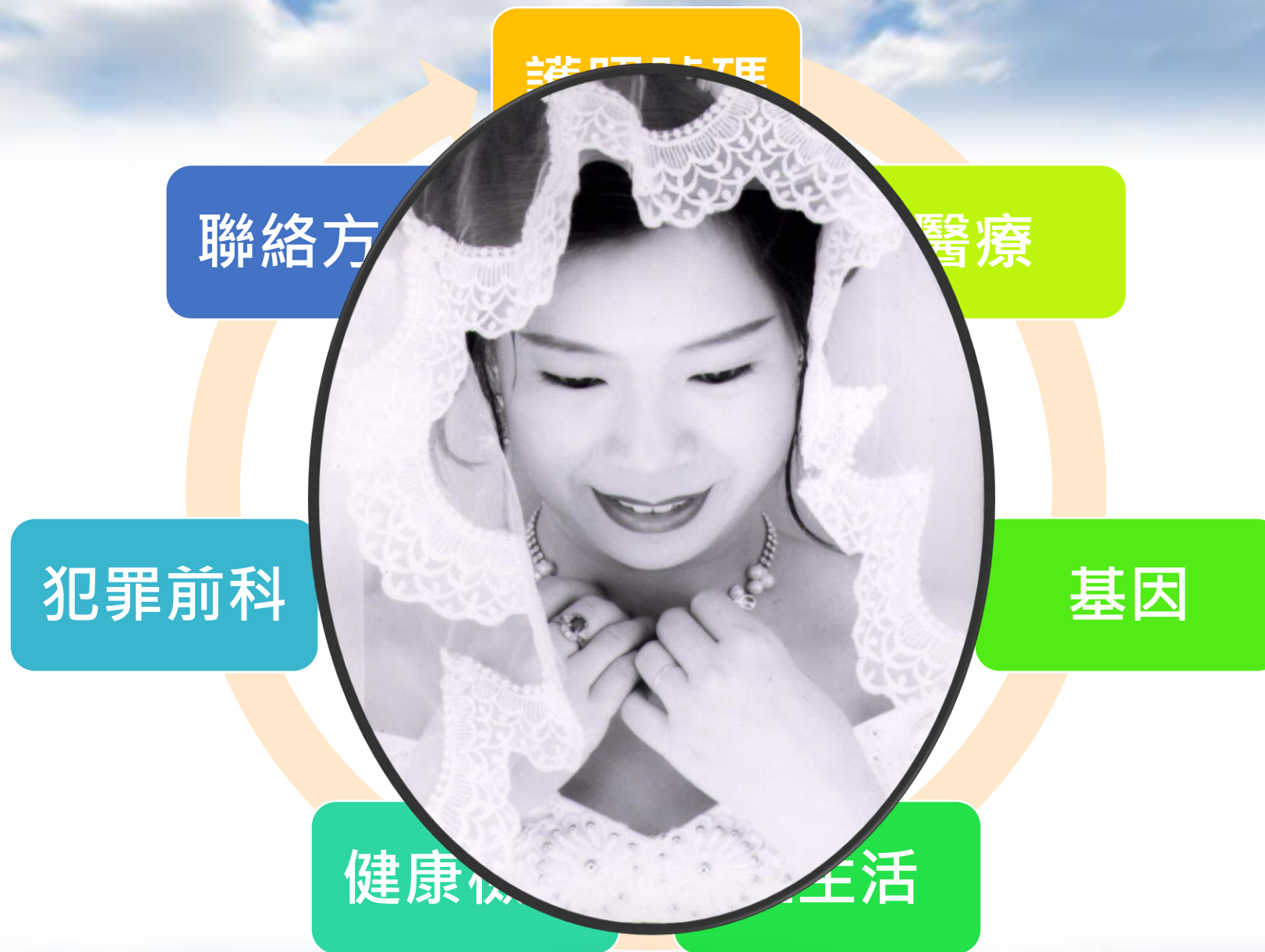


# 直接蒐集

蒐集：指以任何方式取得個人資料



個人資料檔案，包括備份檔案



其他得以**直接**或**間接**方式識別該個人之資料。例如：照片

# 不受保護個資

## 當事人自行公開



☐ 係指當事人自行對不特定人或特定多數人為揭露。

指利用新聞紙、雜誌、政府公報、電子報或其他可供公眾查閱之方式為公開。

## 已合法公開之個人資料



☐ 指依法規公示、公告或以其他合法方式公開之個人資料。



# 間接資料識別

須與其他資料對照、組合、連結

- 楊玉文 N122XXXXXX
- 楊先生 0912-XXX-708



不知為何資料

- 2001:b020:0000:0071:0000:0000:0000:0073
- 112.34.56.67



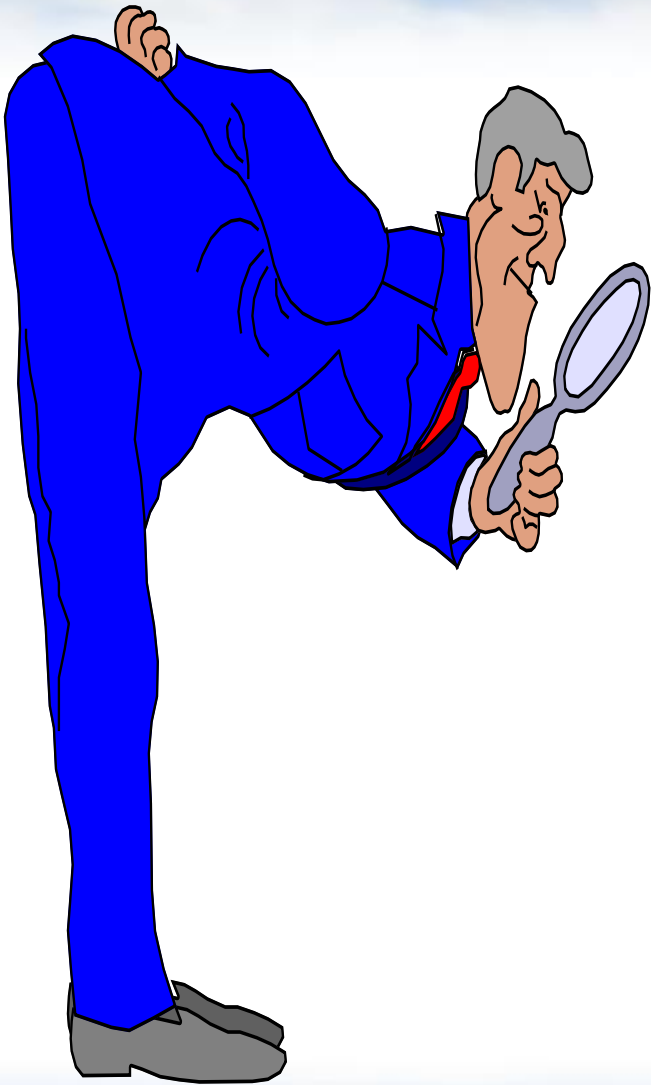
# 處理



輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送

建立或利用個人資料檔案所為資料之記錄

# 利用



指將蒐集之個人資料為處理以外之使用

國內企業只要擁有1筆以上的顧客資料，即符合個資法的規範。

# 安全維護(1)

- 一、成立管理組織，配置相當資源。(專人管理即可)
- 二、界定個人資料之範圍。
- 三、個人資料之風險評估及管理機制。
- 四、事故之預防、通報及應變機制。
- 五、個人資料蒐集、處理及利用之內部管理程序

企業須做的事





# 安全維護(2)

- 六、資料安全管理及人員管理。
- 七、認知宣導及教育訓練。
- 八、設備安全管理。
- 九、資料安全稽核機制。
- 十、必要之使用紀錄、軌跡資料及證據之保存。
- 十一、個人資料安全維護之整體持續改善。

企業須做的事



# 個資罰責

犯本章之罪者，告訴乃論，加重其刑至二分 之一

處新臺幣二萬元以上五十萬元以下罰鍰，限期改正

非公務機關依規定受罰鍰，除能證明已盡防止義務者外，應並受  
同一額度罰鍰之處罰。

# 個資罰責

處**五年**以下有期徒刑拘役

併科新臺幣**一百萬元**以下罰金



公務機關加重二分之一

# 換證留個資

委外守衛A將客戶資料中之一個欄位「**聯絡方式**」賣給廣告業者B，則是否屬個人資料保護法所規範之可識別個人資料。



守衛A

聯絡方式



廣告業者B



# 換證留個資



守衛A

## 理由

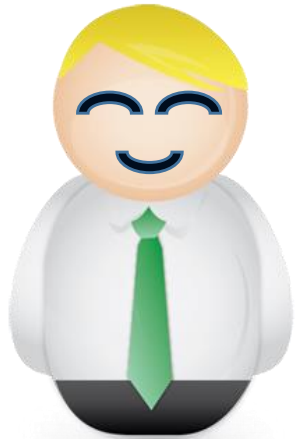
- 「聯絡方式」，守衛掌握換證者的個資，足以識別該特定個人資料。

## 罰責

- 為意圖營利販售可識別之個人資料，故觸犯本法第 41 條第 2 項之刑事構成要件而應負刑事責任。

# 離職員工盜賣個資

離職員工A從企業資料庫，將客戶資料中之一個欄位「聯絡方式」賣給廣告業者B，則是否屬個人資料保護法所規範之可識別個人資料。



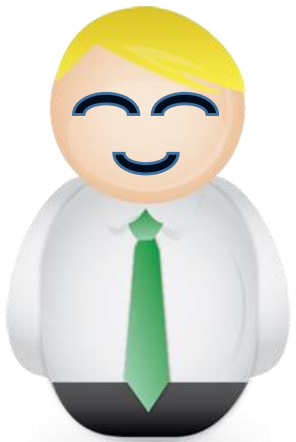
離職員工A

連絡方式



廣告業者B

# 離職員工盜賣個資



離職員工A

## 理由

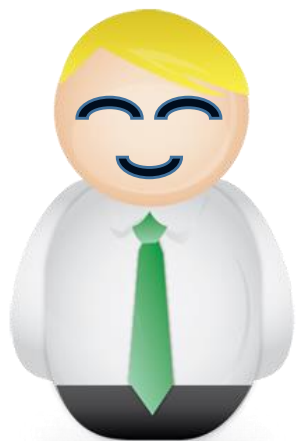
- 「聯絡方式」，可於該企業資料庫之其他資料欄位經對照、組合、連結等間接方式，而能識別該特定個人資料。

## 罰責

- 為意圖營利販售可識別之個人資料，故觸犯本法第41條第2項之刑事構成要件而應負刑事責任(非告訴乃論)。

# 隨身碟儲存個資

職員A坐高鐵時資料掉了(隨身碟)，是否屬個人資料保護法所規範料。



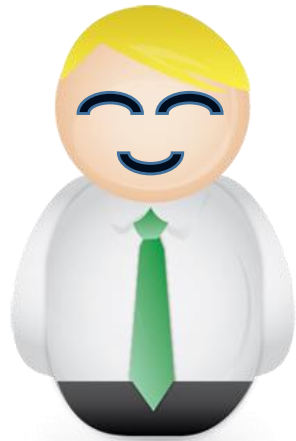
職員A



儲存設備



# 隨身碟儲存個資



職員A

## 理由

- 該「碟身碟」內容，若有明確個資，需個案認定

## 罰責

- 適用個人資料保護法刑責(無故意過失)

個人認為視檔案資訊而定與是否有加密等作為



# 企業應有的作為



企業

## 理由

- 員工個人行為，造成企業損失

## 罰責

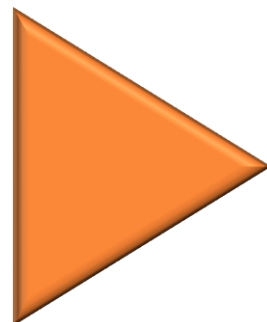
- 適用個人資料保護法(無故意)
- 應重新檢視並改善個資保護流程。

# 紙本文件管理

專人管理



浮水印



保險箱

# 紙本個資防護

- 影印
- 歸檔
- 簽名



# 紙本個資防護

1. 保留列印資訊
2. 數位影像存證
3. 紙本文件加註
4. 搭配**RFID**保護識別





# 認識資安

- 在電腦上運用各種管理程序及防護技術
- 以確保資料的安全
- 避免被他人讀取或修改
- 造成損失





# 駭客鎖定



玉山銀行  
(2010)

卷商遭駭  
(2016)



一銀盜領  
(2016)

遠銀被駭  
(2017)

# DDOS攻擊

- **2017.01** 全台**13**家券商遭到**DDoS**勒索攻擊，要求支付**7~10**個比特幣，元大、亞東、大展....等多家券商受害
- **2016.07** 第一銀行爆發**ATM**盜領案



# 攻擊趨勢

## DDoS攻擊

- 全名 ( **Distributed Denial of Service**)
- 是一種分佈式拒絕服務
- 目的是讓指定目標無法提供正常服務

# 認識APT

英文全名：**Advanced Persistent Threat**、中文是進階持續性滲透攻擊的意思



**RSA**、**Sony**為**APT**攻擊 損失慘重的目標。

# 網路釣魚

特定  
目標

電子  
郵件

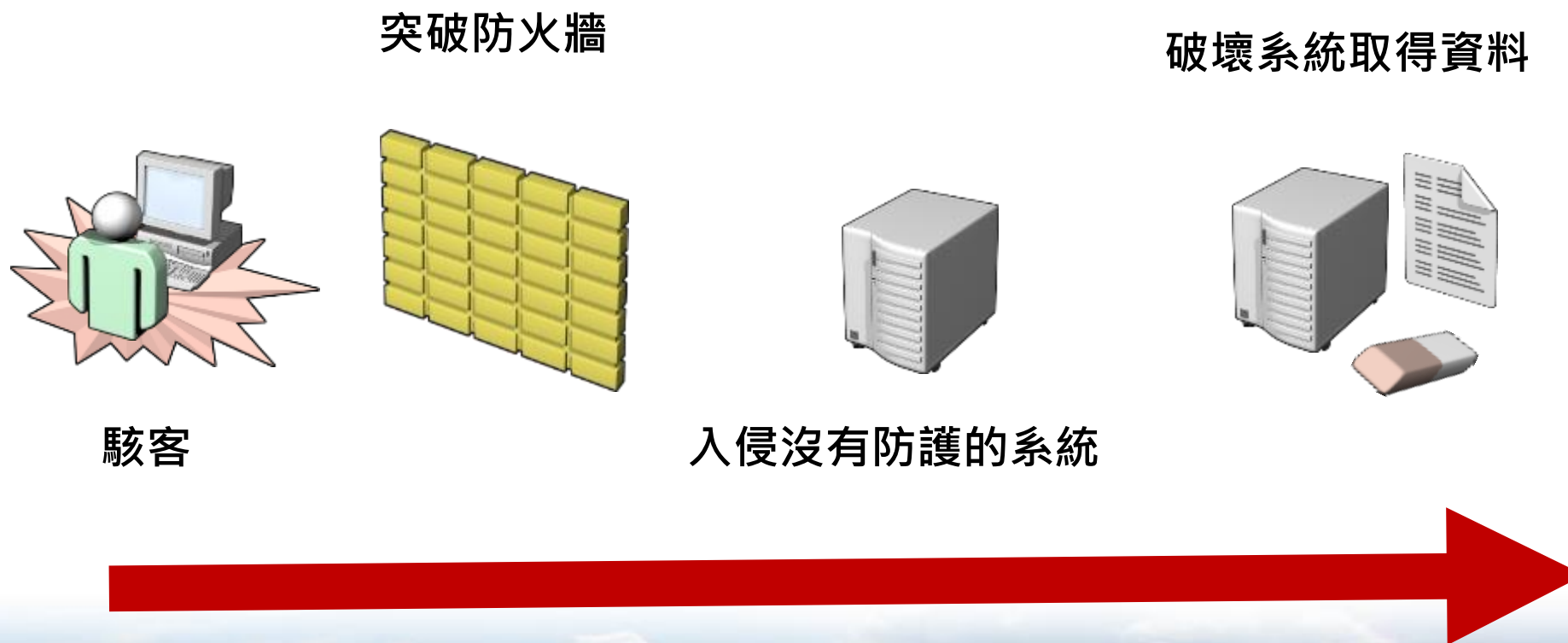
假冒  
名義

植入  
間諜

竊取  
機密



# APT攻擊流程



# APT攻擊

可能來自\_\_\_\_\_



北韓



中國



俄羅斯

資料來源：美國FireEye

# 個資洩因素

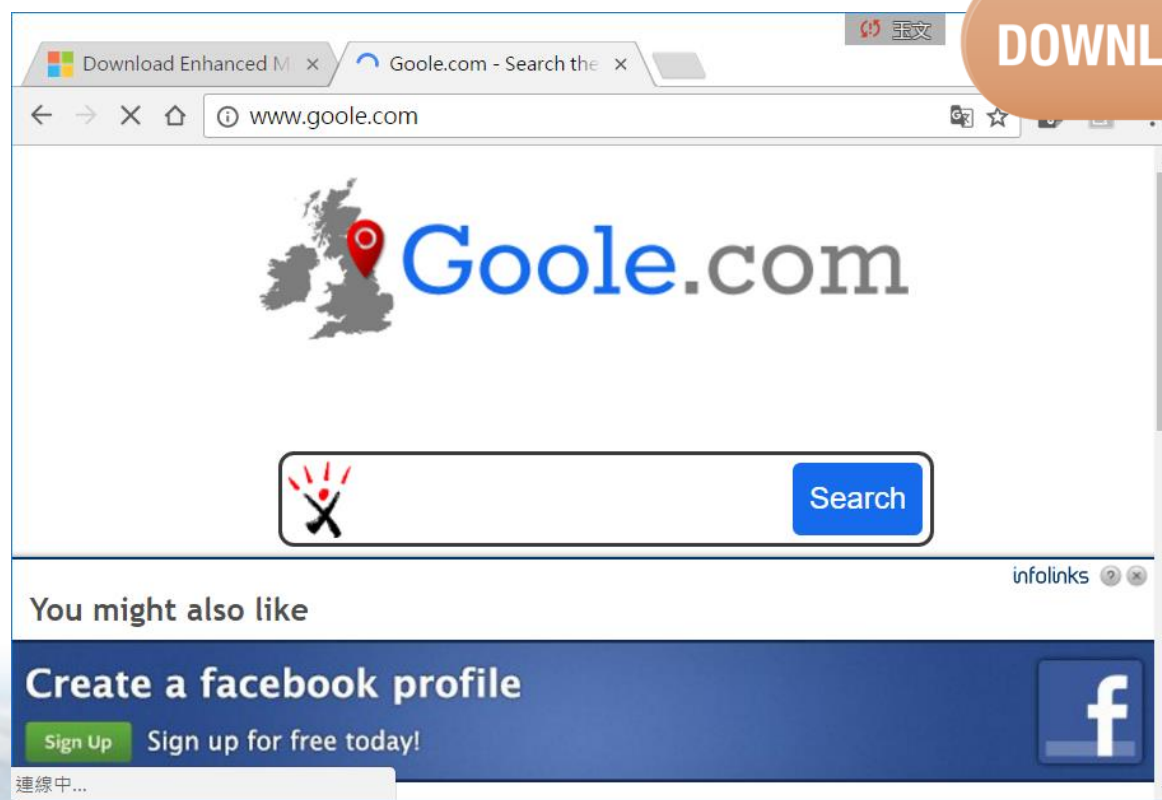
磁碟存取

任意下載

網站瀏覽

社群留言

資料上傳



DOWNLOAD



# 個資防護作法



檔案加密



文件備份



列印輸出



權限管理

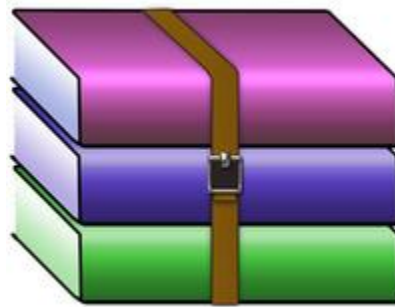


上傳雲端

# 檔案部份



檔案加密

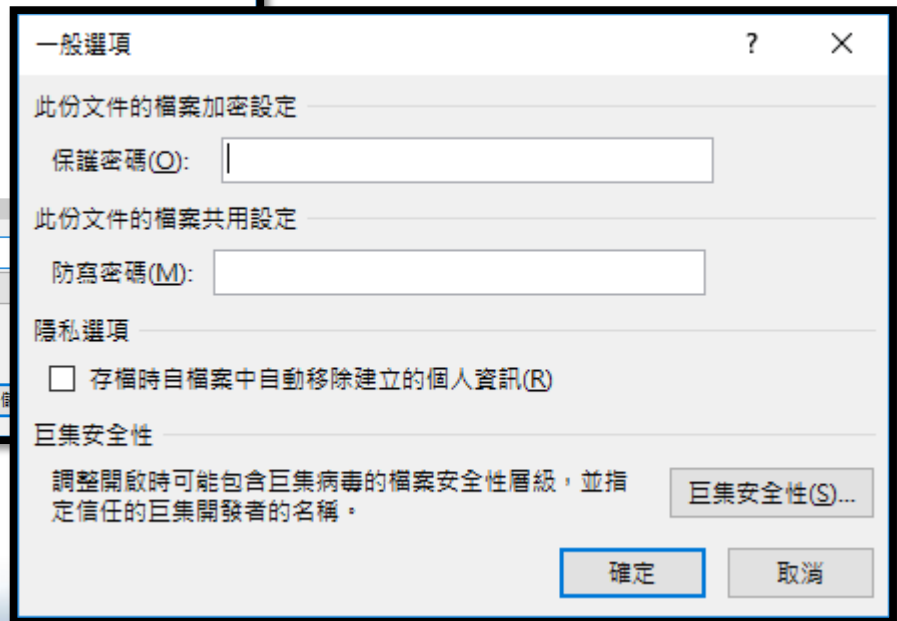
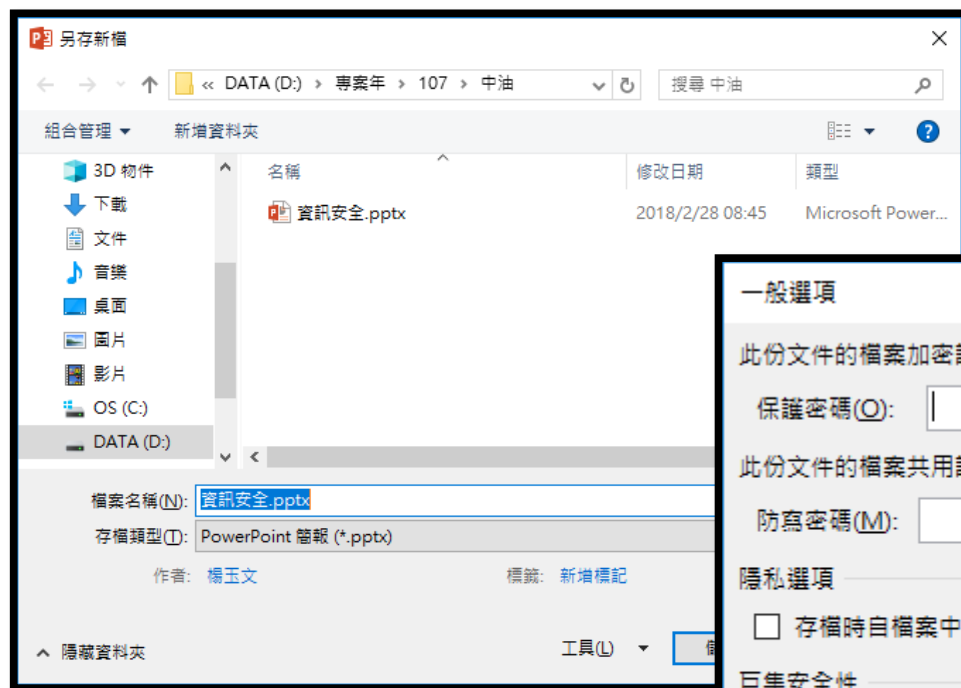


壓縮加密



# 檔案加密

1. 另存新檔
2. 工具
3. 一般選項



# USB磁碟運用

停止  
AUTORU  
N.INF啟動

使用前對  
隨插即用  
裝置掃毒

不執行裝  
置內可疑  
檔案

勿用全選  
備份 (隱性  
檔案)

# 隨身碟加密(檔案)

## • BITLOCKER



# 隨身碟使用原則

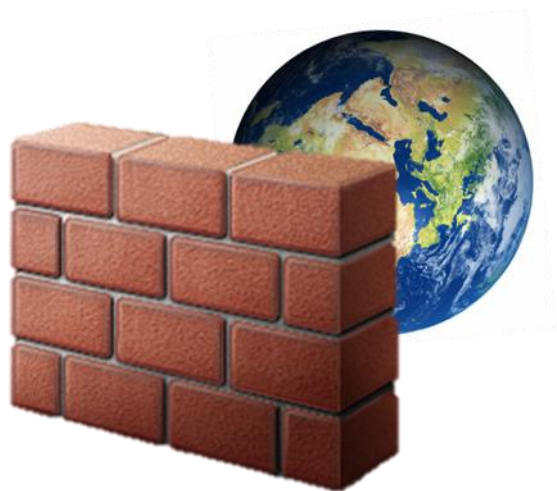
隨身碟要加密【檔案、資料夾】

移除時使用安全移除

不要讓他人你的電腦上任意使用隨身碟



# 系統部份



防火牆啟用



防毒軟體

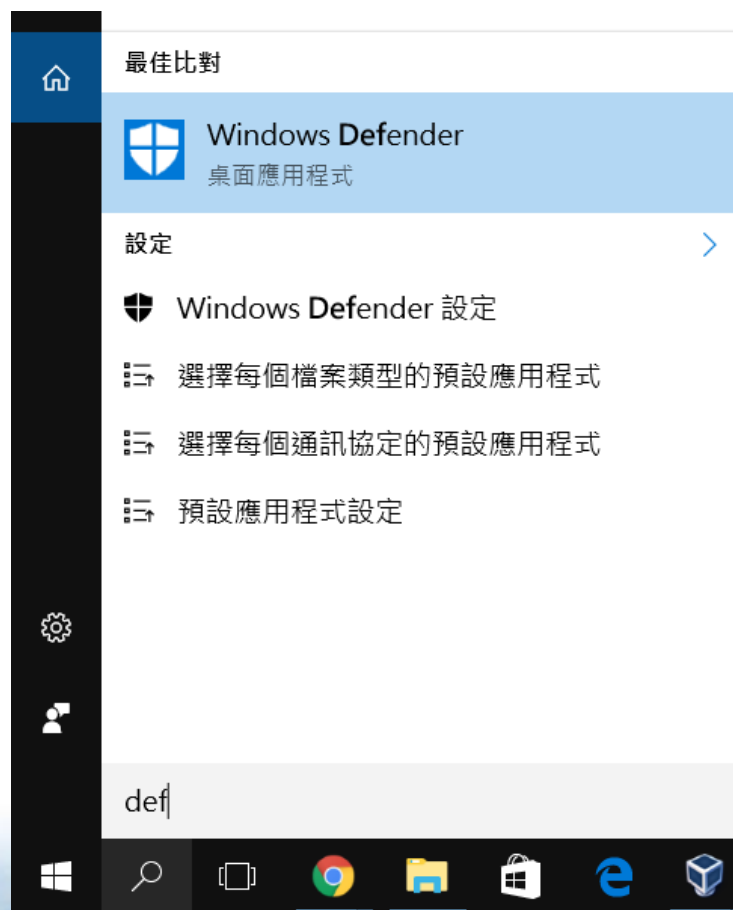


UAC設定



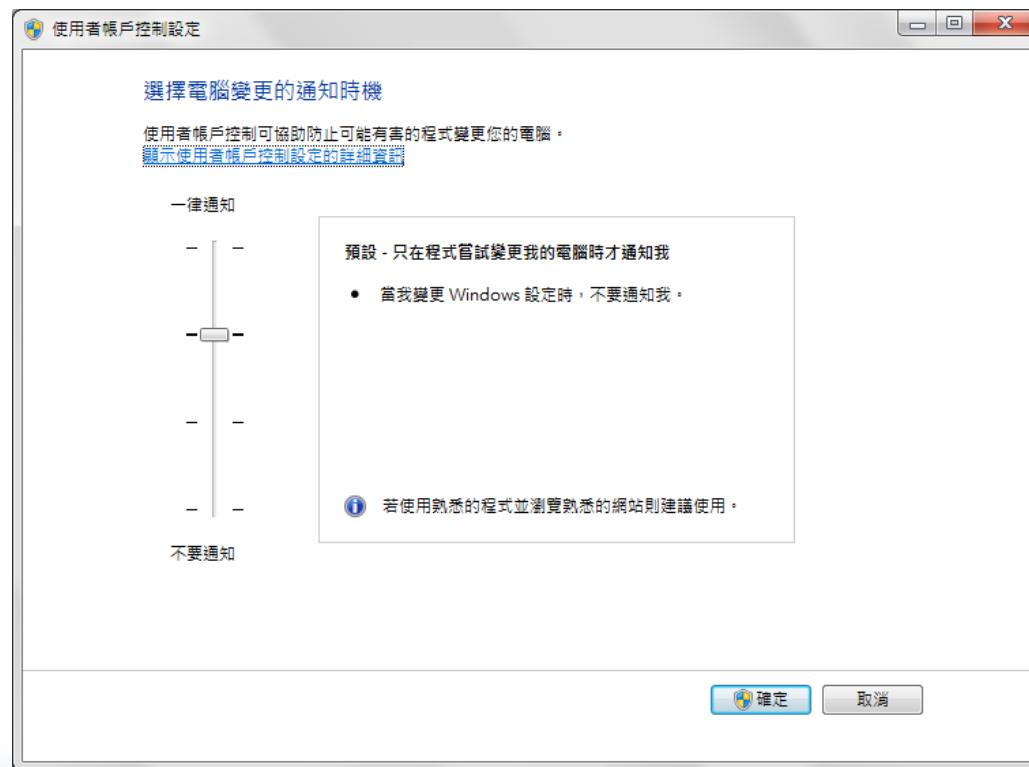
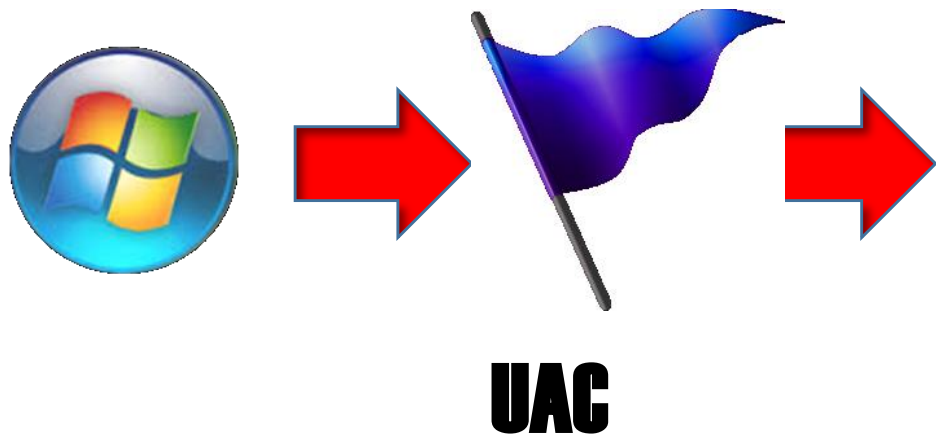
# 系統檢測

## Windows Defender：檢測惡意木馬程式



# 權限管理

## 使用者帳戶控制



# 網路部份

注意  
網址

掃描  
軟體

停用  
下載

不儲  
密碼

# 釣魚郵件

拍賣  
信件

會員  
通知

廣告  
郵件

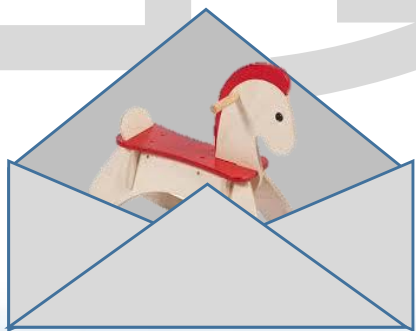
偽造  
信件

# 木馬信件



- 利用電子郵件的郵件內容或附件
- 如啟用自動預覽功能，即感染木馬程式。

個資外洩



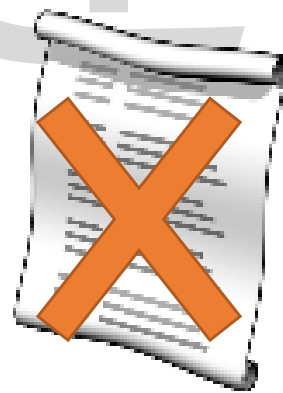
中毒





洩外資個

錯誤連接



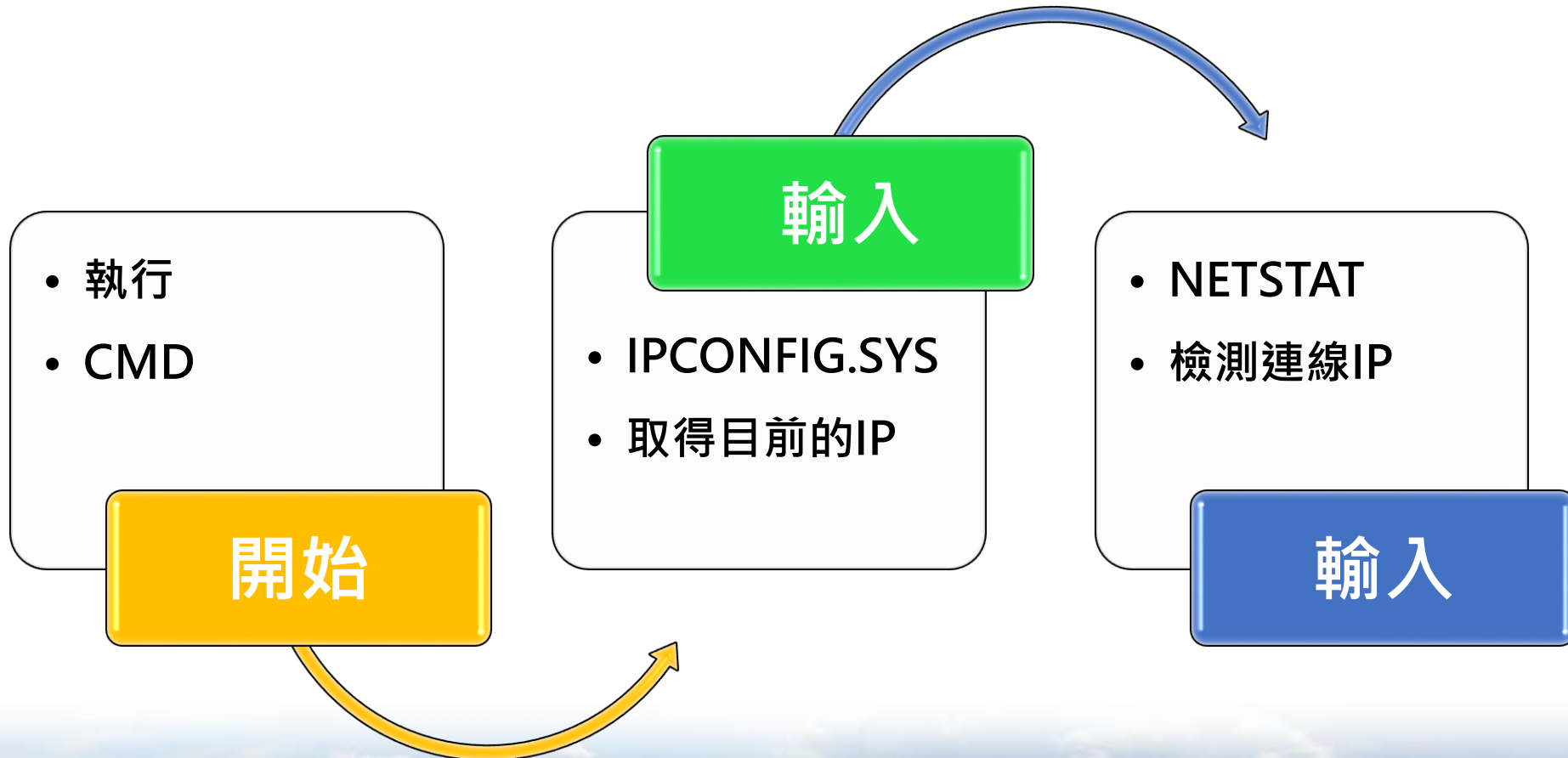
不知名網頁

# 郵件防護策略

- 不於任何公開的場所，收發郵件
- 不開啟來歷不明之郵件
- 不轉寄非必要之郵件
- 不回應任何未知的郵件



# 上網前的預防



# 使用者帳戶

## 瀏覽器帳戶



# 網路廣告

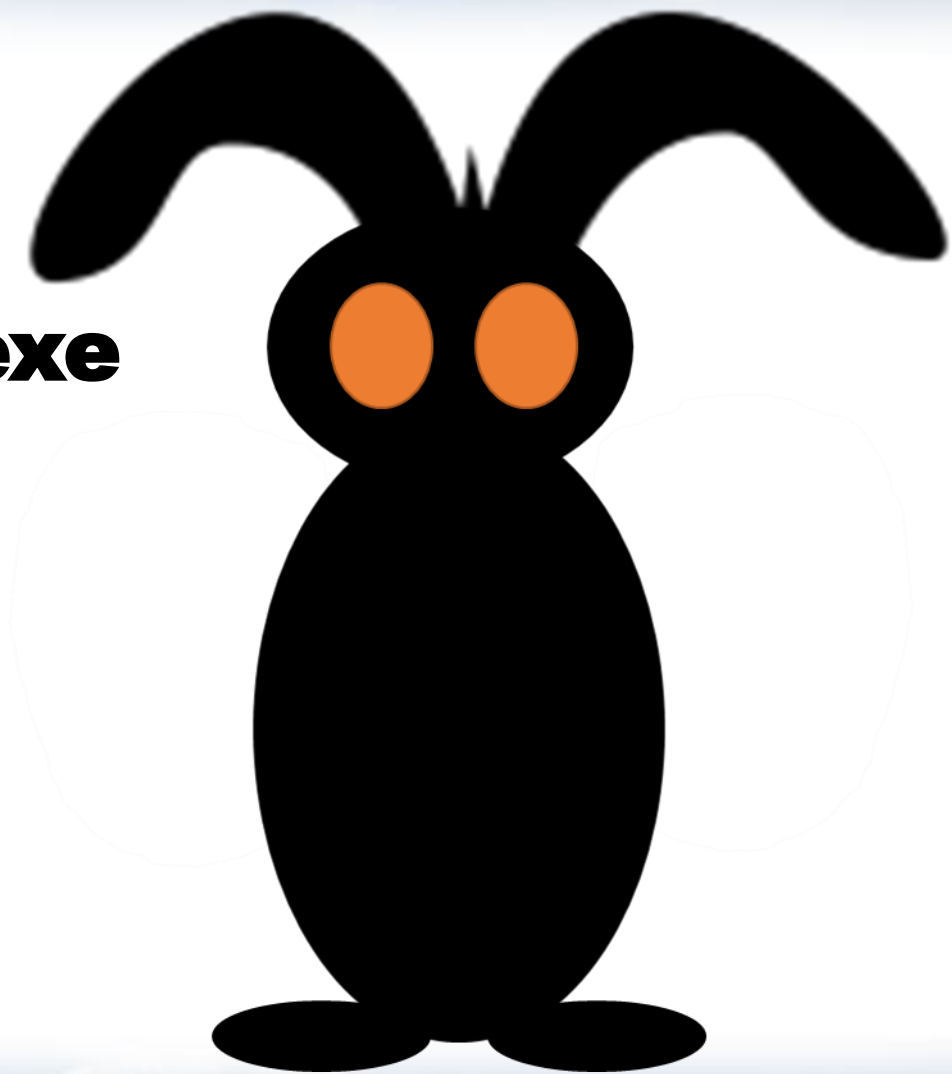


1. 惡意網頁廣告盜取個資
2. 只要瀏覽器或裝置顯示出惡意廣告，就會受到攻擊



# BadRabbit

- **Petya** 變種
- 要求安裝**install\_flash\_player.exe**
- **dispci.exe**
- 檢查一下防火牆設定



# 以照易物



MalwareHunterTeam

nRansomware



裸照



解鎖密碼



Deep Web販售

深網



他們真正的目的是什麼

# 防範挖礦

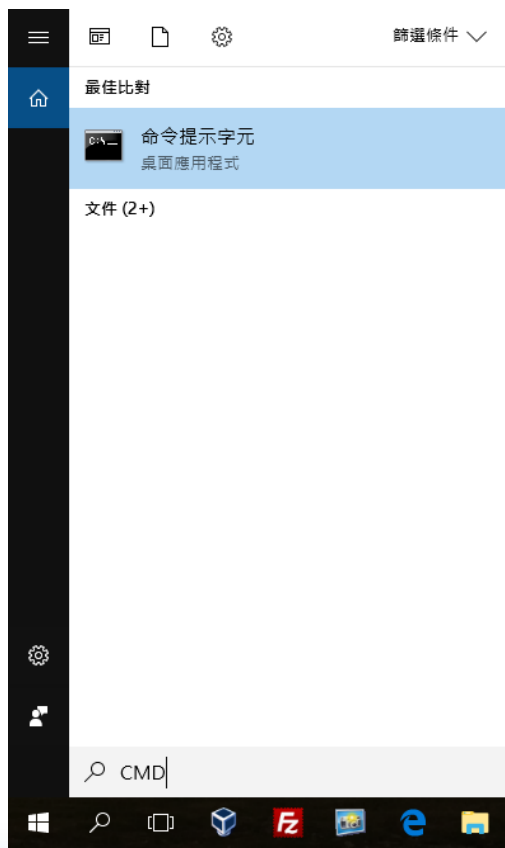
## 擴充程式(Coin-Hive Blocker)



資料來源：趨勢科技

# 惡意中繼站IP

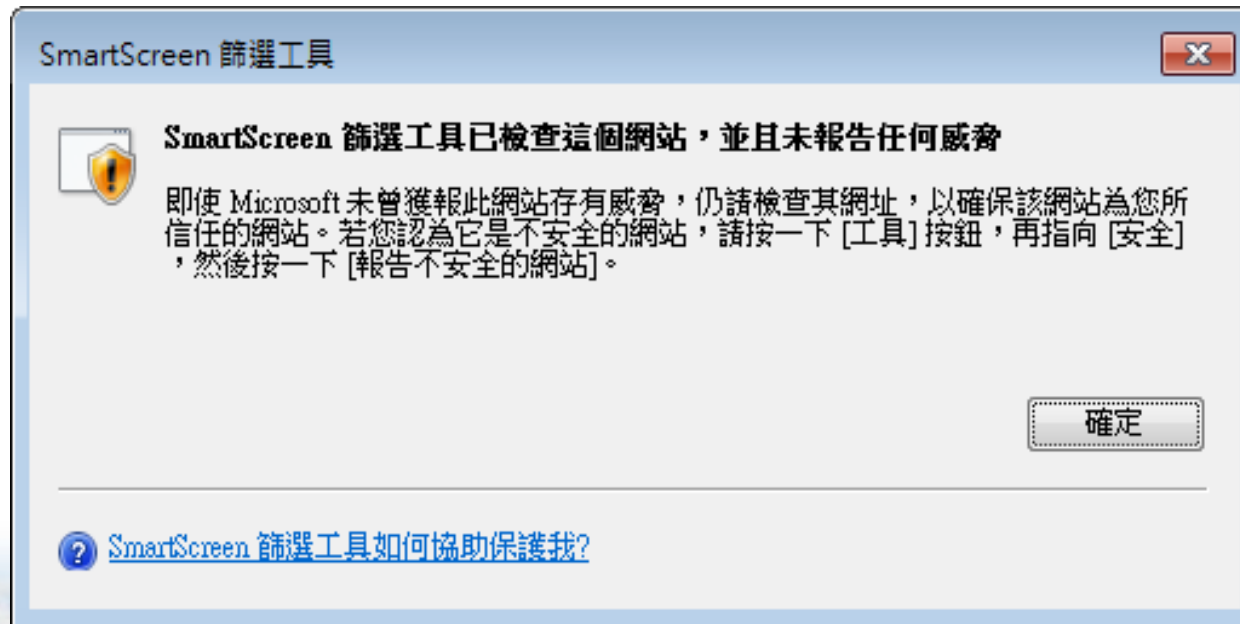
- **CMD**
- **NETSTAT**



94.23.148.41  
167.114.32.112

資料來源：iThome

# 進網站的預防





# 不可下載

- 無須安裝可立即執行，故稱為「免安裝」

可攜式

不寫入

免費



# 檢測遭害



bitsran.exe  
RSW72CE.Tmp  
msmpeng.exe  
splwow32.exe  
FileTokenBroker.dll

資料來源：iThome

工作管理員

檔案(F) 選項(O) 檢視(V)

處理程序 效能 應用程式歷程記錄 開機 使用者 詳細資料 服務

名稱	PID	狀態	使用者名稱	CPU	記憶體 (私...)	描述
esif_uf.exe	3508	執行中	SYSTEM	00	1,300 K	Intel(R) Dynamic Platform and ...
EvtEng.exe	3500	執行中	SYSTEM	00	3,740 K	Intel(R) PROSet/Wireless Event...
explorer.exe	524	執行中	alexmysir	00	19,632 K	Windows 檔案總管
fontdrvhost.exe	940	執行中	UMFD-0	00	2,456 K	Usermode Font Driver Host
fontdrvhost.exe	11084	執行中	UMFD-26	00	5,908 K	Usermode Font Driver Host
GoogleCrashHandl...	10812	執行中	SYSTEM	00	116 K	Google Crash Handler
GoogleCrashHandl...	10900	執行中	SYSTEM	00	116 K	Google Crash Handler
GoogleUpdate.exe	12740	執行中	SYSTEM	00	560 K	Google 安裝程式
IAStorDataMgrSvc...	6272	執行中	SYSTEM	00	32,284 K	IAStorDataSvc
IAStorIcon.exe	5848	執行中	alexmysir	00	8,856 K	IAStorIcon
ibtsiva.exe	3476	執行中	SYSTEM	00	900 K	Intel(R) Wireless Bluetooth(R) i...
igfxCUIService.exe	1916	執行中	SYSTEM	00	1,520 K	igfxCUIService Module
igfxEM.exe	12512	執行中	alexmysir	00	2,540 K	igfxEM Module
IntelCpHDCPSvc.exe	3492	執行中	SYSTEM	00	960 K	Intel HD Graphics Drivers for ...
IntelCpHeciSvc.exe	4348	執行中	SYSTEM	00	1,188 K	IntelCpHeciSvc Executable
jhi_service.exe	8232	執行中	SYSTEM	00	908 K	Intel(R) Dynamic Application L...

較少詳細資料(D) 結束工作(E)

# 結束網站

工具



網際網路選項



結束刪除瀏覽  
記錄

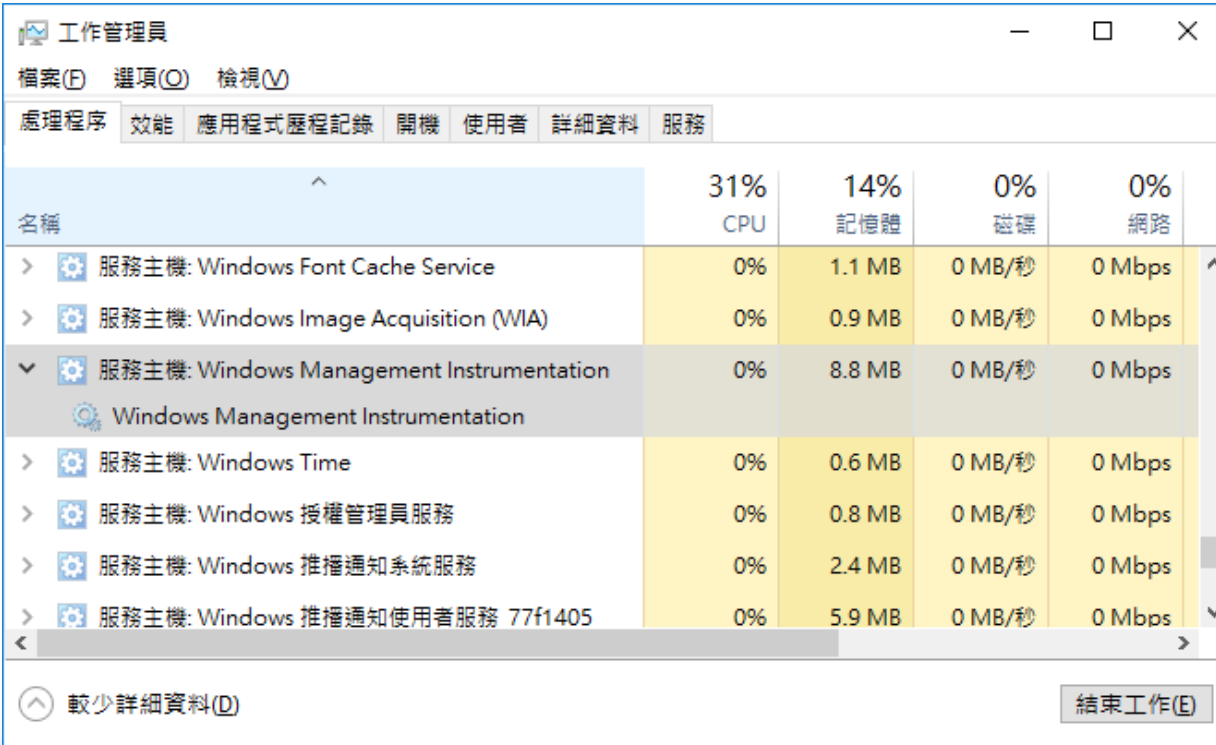


# 伺服器遭挾持挖礦

受害國家排名：俄羅斯、印度、**台灣**

1. 永恆之藍（EternalBlue）攻擊工具
2. 變成入侵 Windows 伺服器的「Smominru」有害程式
3. 透過WMI散播(Windows Management Infrastructure)

## WannaCry



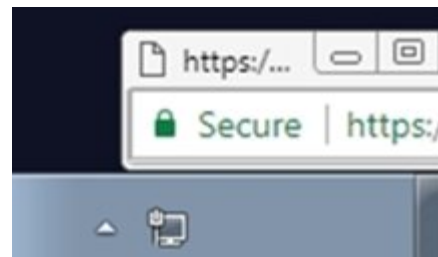
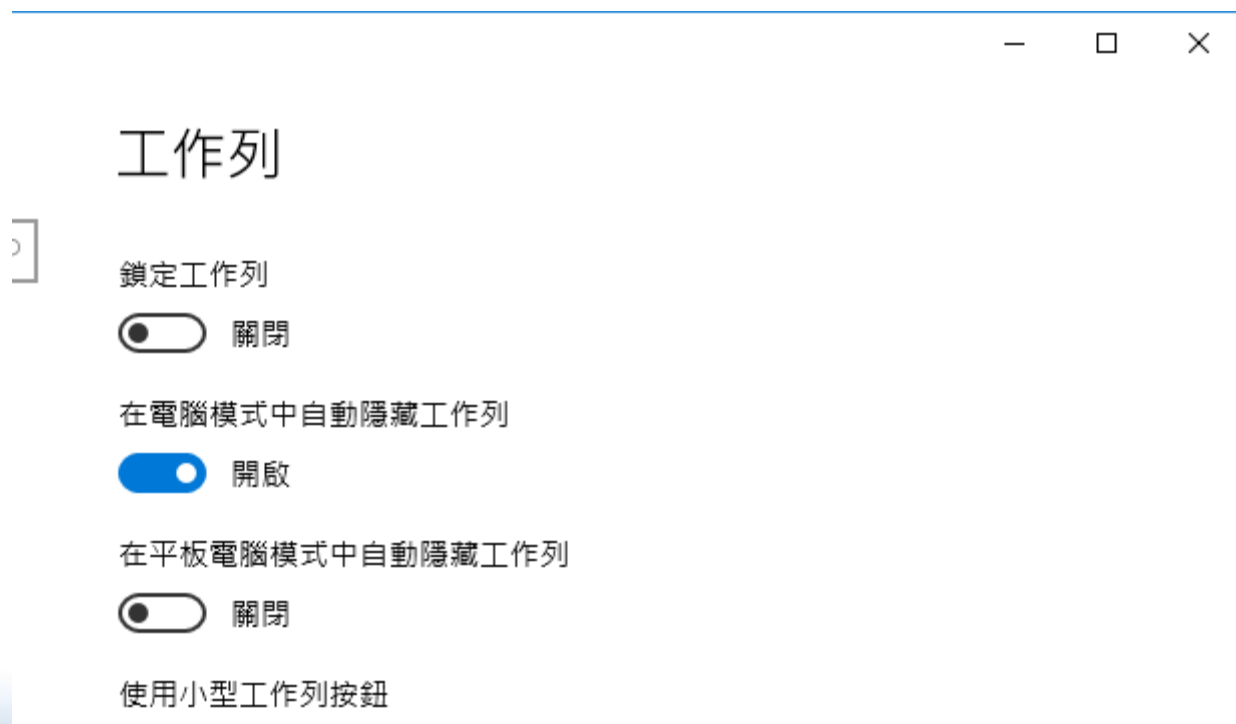
工作管理員				
檔案(F) 選項(O) 檢視(V)				
處理程序 效能 應用程式歷程記錄 開機 使用者 詳細資料 服務				
名稱	31% CPU	14% 記憶體	0% 磁碟	0% 網路
> 服務主機: Windows Font Cache Service	0%	1.1 MB	0 MB/秒	0 Mbps
> 服務主機: Windows Image Acquisition (WIA)	0%	0.9 MB	0 MB/秒	0 Mbps
▼ 服務主機: Windows Management Instrumentation	0%	8.8 MB	0 MB/秒	0 Mbps
Windows Management Instrumentation				
> 服務主機: Windows Time	0%	0.6 MB	0 MB/秒	0 Mbps
> 服務主機: Windows 授權管理員服務	0%	0.8 MB	0 MB/秒	0 Mbps
> 服務主機: Windows 推播通知系統服務	0%	2.4 MB	0 MB/秒	0 Mbps
> 服務主機: Windows 推播通知使用者服務 77f1405	0%	5.9 MB	0 MB/秒	0 Mbps

較少詳細資料(D) 結束工作(E)

資料來源：Proofpoint

# 2500網站挖礦

隱藏工具列之後，設定【自動隱藏】



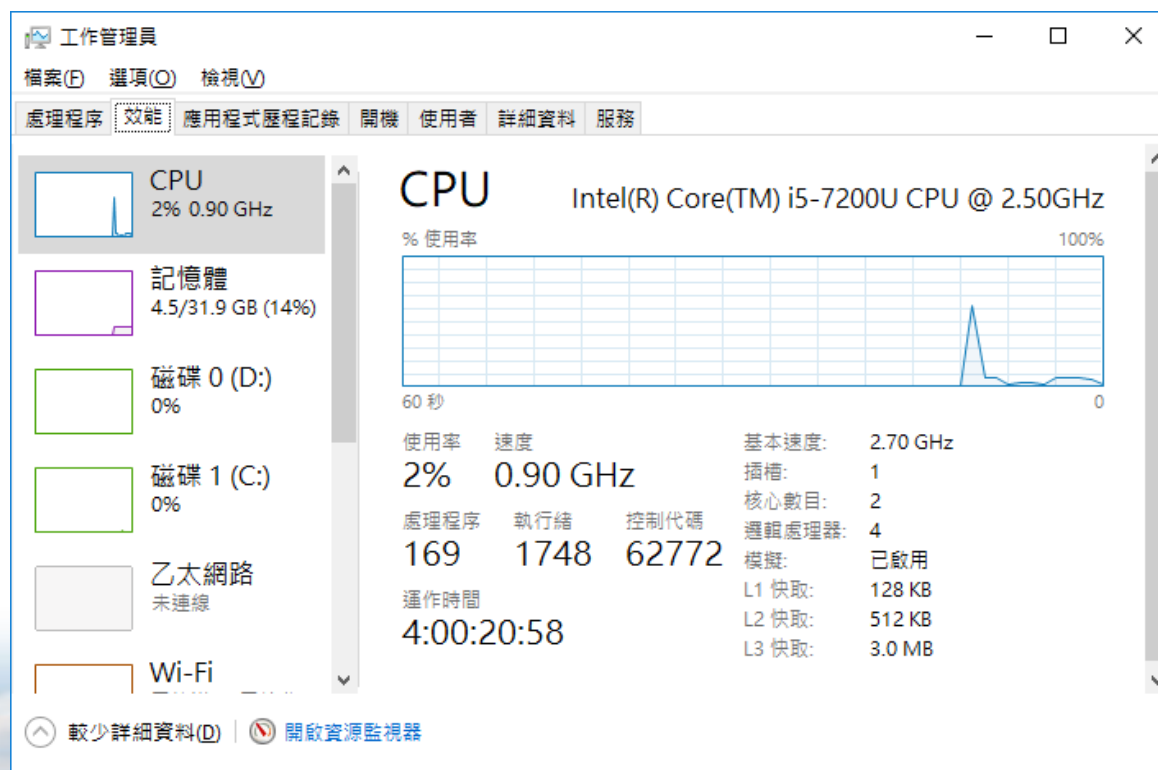


# 檢測是否淪為挖礦

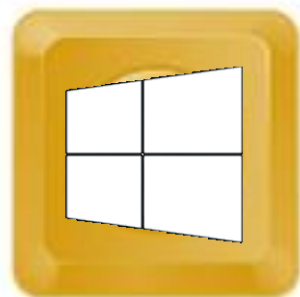


採礦平台 Coinhive 的原理  
就是利用 JavaScript 挖礦  
coinhive.min.js

CPU效能約**56%**



# 離座管理 離席 保護



楊玉文

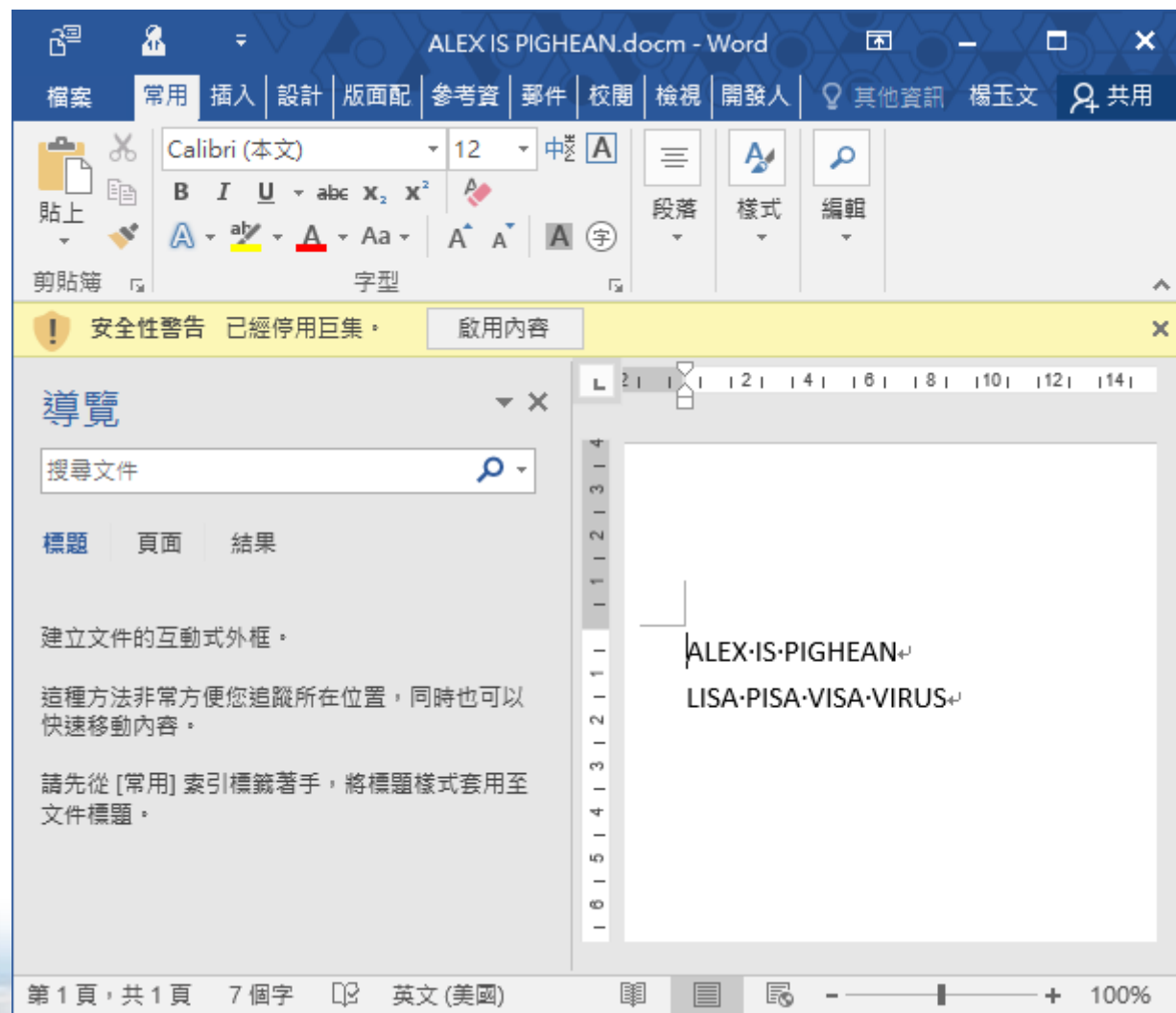
密碼



# Word文件勿亂啟用

- 最新的**Win32**病毒植入**dropper**
- 躲過**Windows**的驗證機制
- 冒充**Word**的文件
- 會以文件受到保護，要求使用者同意「啟動內容」

資料來源：McAfee



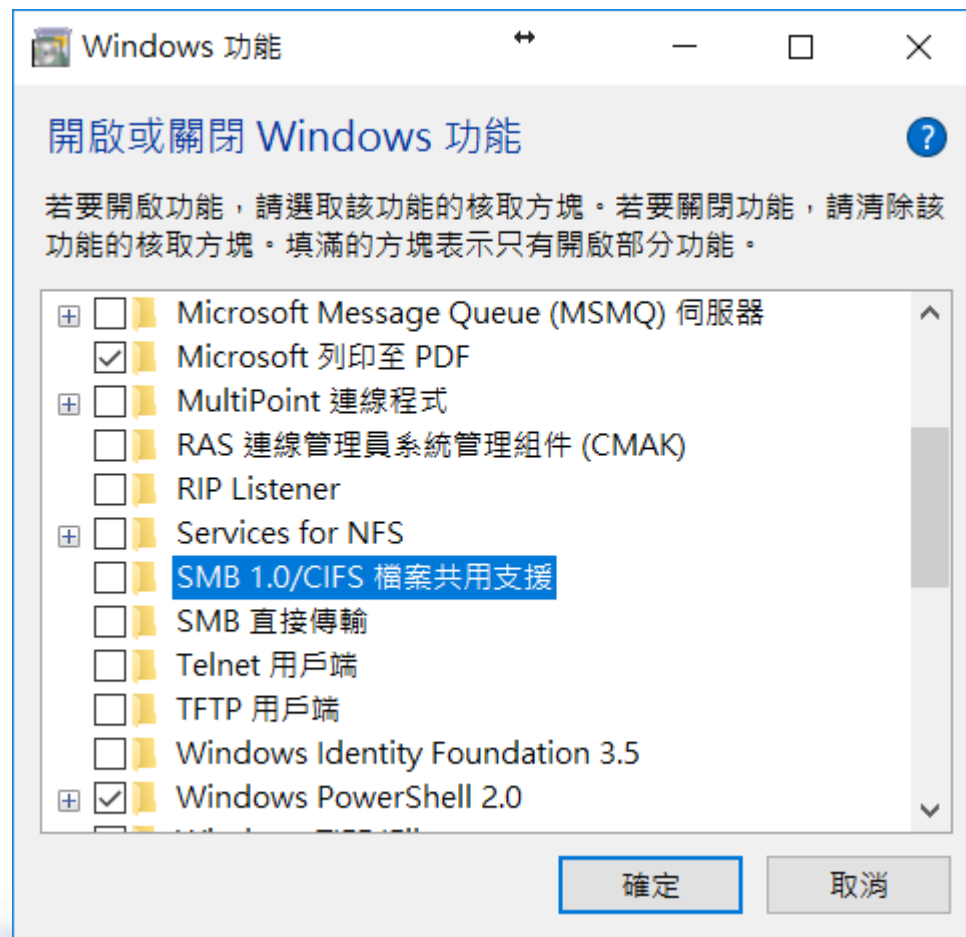


# 停用SMB

關閉 Windows 功能

關閉 SMB 1.0

CIFS 檔案共用支援



# 系統更新



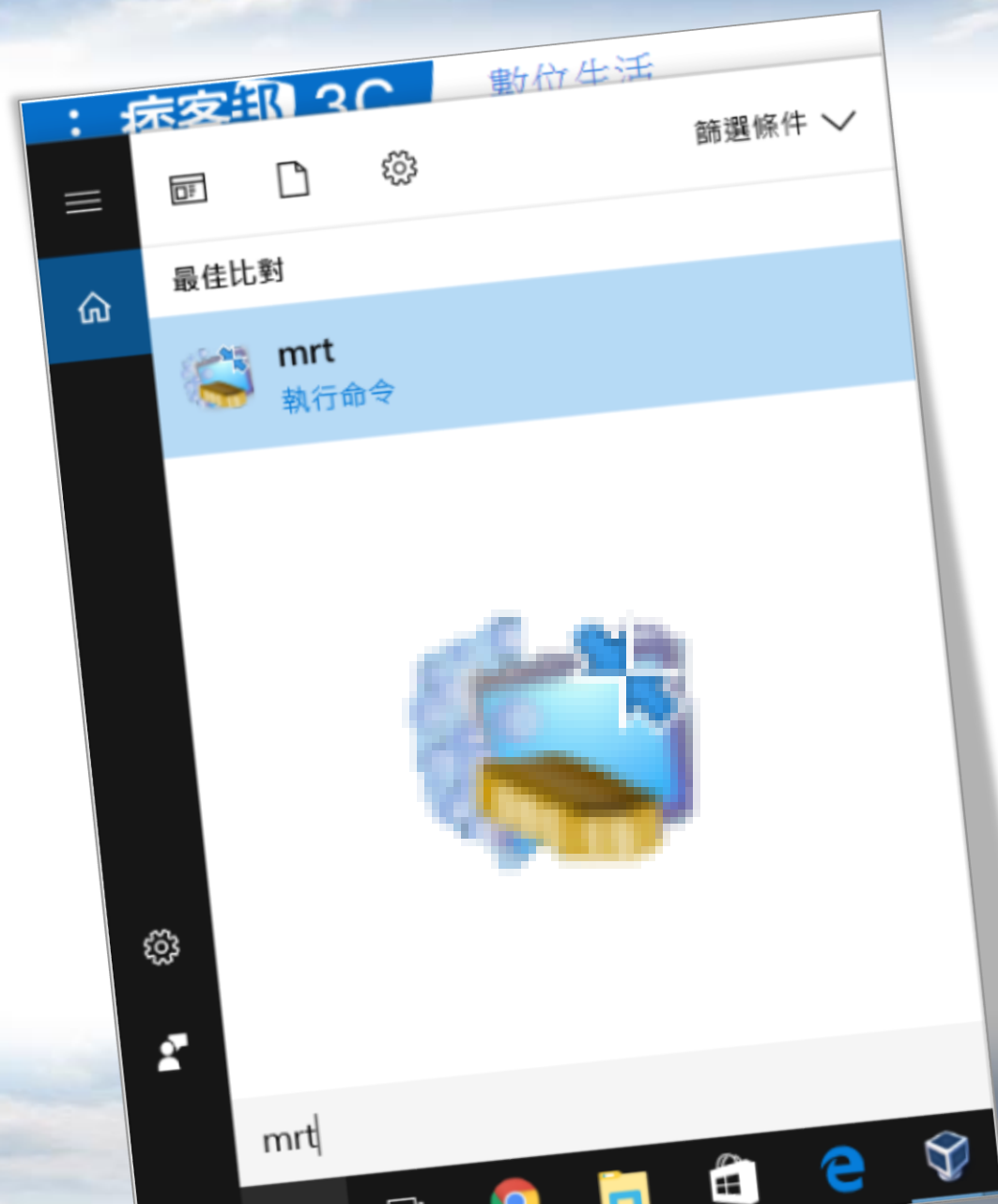
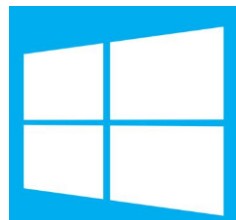
Windows 10





# 系統防護

1. 開始
2. 尋找
3. 輸入mrt



# 資料備份

企業備份

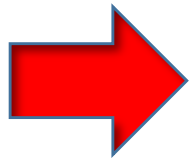


# 強化網路安全

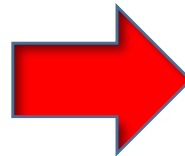
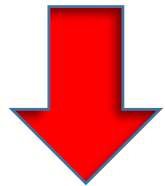
檢出異常 有可能遭受測錄



CMD



NETSTAT



**netstat /a | find "LISTENING"**

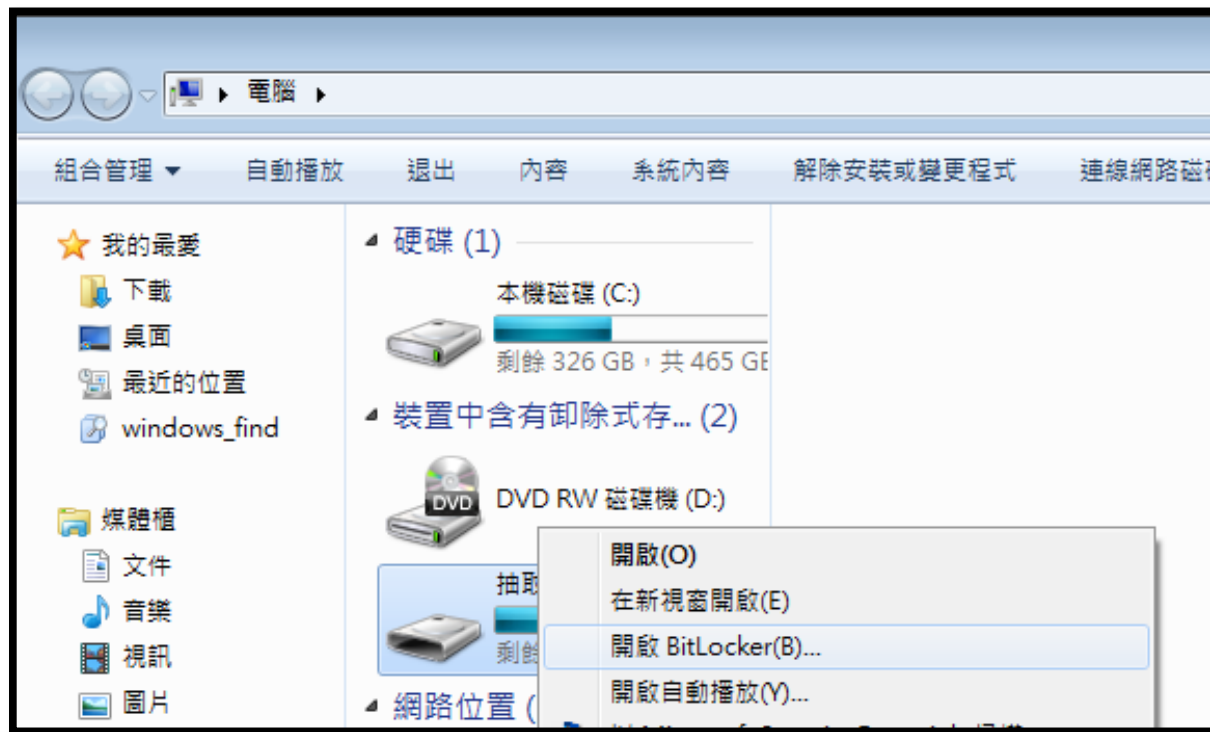
```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\alexsir>netstat /a | find "listening"

C:\Users\alexsir>
```

# 強化安全

## • BITLOCKER



# 強化網路安全

- 防火牆保護
- 隔離外部及內部網路
- **Proxy Server**存取





# 行動個資風險

1. 美國中央情報局 ( CIA )
2. 國家安全局 ( NSA )
3. 聯邦調查局 ( FBI )
4. 國防情報局....6大機構

資料來源：自由時報

資  
安  
疑  
慮



# APP個資外洩



趨勢科技官方發文：交友軟體Tinder 透過Facebook、Spotify取得個資，目前已修補完成。

電話號碼註冊



Tinder

# 關閉前鏡頭



相機阻擋

1. 防止間諜程式，流氓軟體與病毒程式
2. 使用手機上拍攝未經授權的照片與錄影



# RedDrop

## 新型的Android系統內建53個APP

1. 聯絡人和相簿
2. 即時盜錄
3. 簡訊付費
4. 網路數據
5. 盜取Wi-Fi資訊

資料來源：Wandera





# RedDrop

## 新型的Android系統內建53個APP

1. 目標是提取有價值、有害的數據
2. 攻擊者會用於敲詐勒索
3. Dropbox、Drive文件夾要注意
4. YL\_PLUGIN.APK、C3B92.30106.JAR

資料來源：Wandera





# 行動定位



**Android** 設備 **>30萬次** 定位攻擊  
**iOS** 設備亦崩潰



# 藍芽連線



不用配對或設定就能駭入裝置  
受影響作業系統

1. **Android**
2. **Linux**
3. **Windows**
4. **iOS 10**以前的系統

資料來源：**Armls**資安公司

# Wifi連線

- **FREE** 別亂連**WPA2**
- 系統更新 **Android 7.0**、**IOS 11**
- 注意行動裝置是否異常



# 防範方式

- 定期更新系統
- 不下載未知程式
- 隱私設定提高
- 無線網路不亂連
- 小心不請自來的電話或訊息
- 不明來電不回撥





# 好友要小心





# 省電別信

Google Play已移除



1. **Android**系統
2. **EnergyRescue**省電行動程式
3. 被嵌入勒索程式
4. 約**180**美金

資料來源：資安業者Check Point

# 簡訊設定

訊息



設定



多媒體訊息



關閉所有讀取



# 登出不連線

1. 切記要在關閉**APP**時，請選擇「退出帳號」或「登出」
2. 不用手機記錄任何網路買賣的資訊，應使用一般瀏覽器
3. 停用無線網路或**WIFI**自動連接設定



# 充電竊取



# 不用免費

可能竊取照片、簡訊或**E-mail**

資料來源：**Authentic8**資安公司

# 取消同步

- **Android**

- 設定 / 帳號與同步處理
- 自動同步處理

- **iOS**

- 點選每個程式 / 關閉





# 善用APP



警政服務



行動安全防護



ZoneAlarm

# 使用安全

- 啟用手機 **隱私設定**的**阻擋訊息**功能
- 取消 **允許自其他裝置登入**功能
- 不明**連結**不要亂啟用
- 刪除連結（ **goo.gl**、**bit.ly**或**IP**連結
- 勿下載**來源不明未認證**的**APP**程式
- 撥打**165**可求證



# 預防勝於維護

不



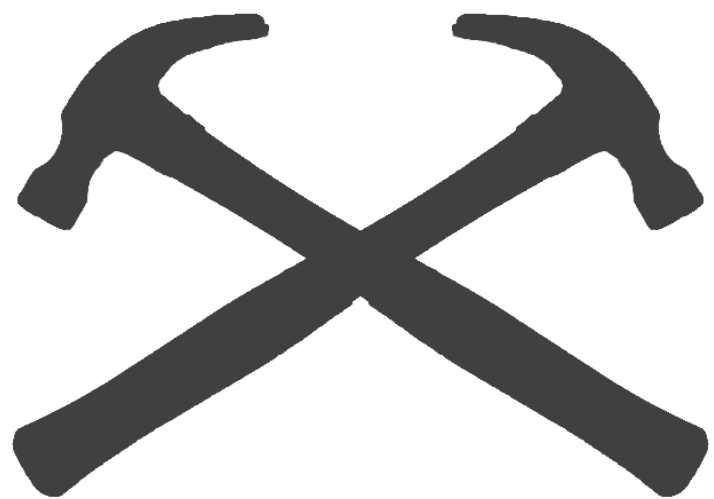
不



不



# 結語



只要全面戒備  
資安就零風險

謝謝指教