

近期資安威脅趨勢

行政院國家資通安全會報 技術服務中心

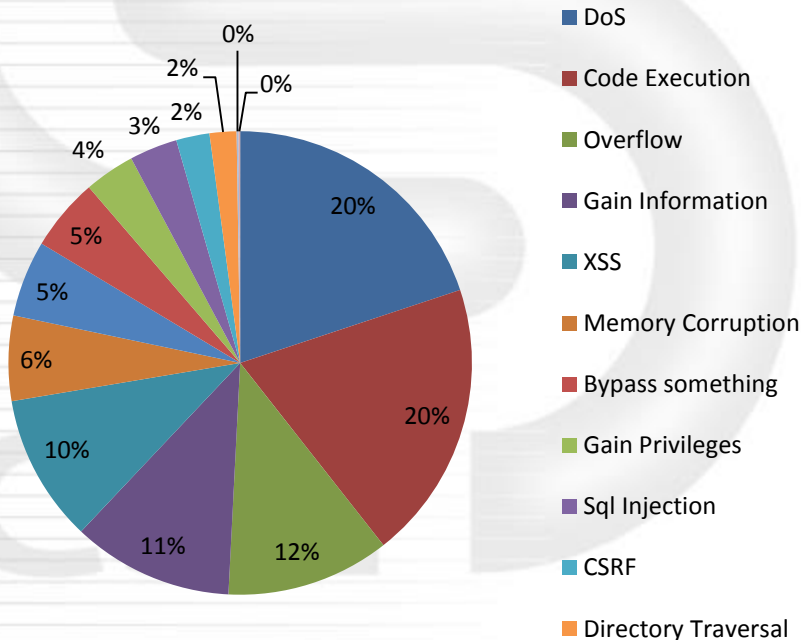
- 前言
- 沒錢就搗蛋的勒索軟體肆虐
- 衛星導航系統引發安全隱憂
- NFC卡便捷但個資要留意
- 結論與建議

● CVE弱點統計資訊

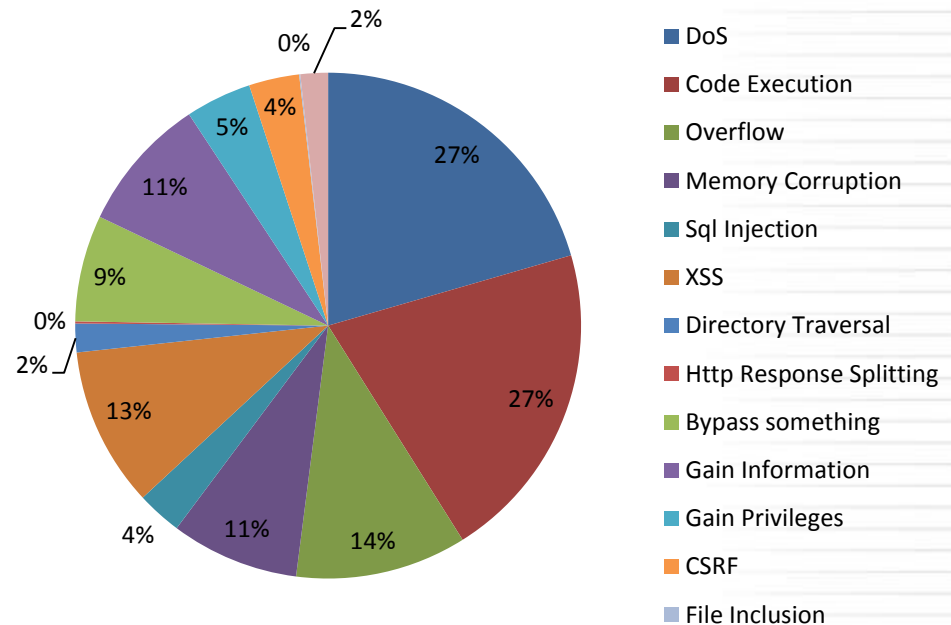
—弱點類型分布

➤ DoS與Code Execution為主要的弱點類型。

2011年~2015年弱點類型分布



2015年弱點類型分布



● 研析2014年~2015年所發生的重大弱點

- Heartbleed弱點
- Logjam及Freak弱點
- GNU Bash Shellshock弱點
- POODLE弱點
- Bugzilla弱點
- HTTP.sys弱點
- Adobe Flash Player零時差弱點
- WinRAR v5.21 SFX零時差弱點
- Joomla存在資料隱碼攻擊漏洞
- 微軟Office檔案格式轉換程式弱點
- 微軟Word堆疊溢位弱點
- 微軟Word RTF記憶體損毀弱點
- 微軟IE存取已刪除或錯置記憶體內容弱點
- 微軟Windows OLE遠端執行程式碼弱點
- 微軟安全通道遠端執行程式碼漏洞
- 微軟Kerberos KDC弱點
- Skype Server和Lync Server弱點

● 蒐集分析重大資料外洩事件(2014年~2015年)

- Snapchat近460萬名用戶資料外洩
- 南韓1.04億筆信用卡個資外洩
- 線上群眾募資平台Kickstarter被駭
- eBay用戶帳密資料庫遭駭
- 好萊塢上百女星私密照外洩
- 美國大型醫療體系CHS遭中國駭客攻擊
- Dropbox用戶資料外洩
- 索尼影業遭到駭客入侵
- 丹堤咖啡遭駭，5000筆會員個資外洩
- 密碼管理服務商LastPass遭駭客入侵
- 資安廠商Hacking Team遭駭客入侵
- 全球知名偷情網站Ashley Madison被駭
- 駭客集團竊取企業未發布財報牟利
- 日本國民年金機構外洩125萬筆個資
- 資安業者Bitdefender遭駭
- Experian遭駭客入侵
- 美國Excellus藍盾藍十字遭入侵
- 音樂群眾集資網站Patreon遭駭
- 美國Scottrade證券遭駭
- 歐悅連鎖精品汽車旅館傳遭駭
- 美國軟體公司在亞馬遜簡易儲存服務外洩150萬筆個人資料

政府機關及金融機構遭駭事件

● 蒐集分析政府機關及金融機構遭駭事件(2014年~2015年)

- 美國摩根年大通銀行遭駭客入侵
- 美國運輸司令部承包商遭中國大陸駭客入侵多次
- 美國白宮網路遭駭客入侵
- 南韓水力與核電公社(KHNP)傳出遭到駭客入侵
- 比特幣交易商Bitstamp遭駭客入侵
- 美軍中央司令部社群網路帳號遭駭客入侵
- 美國國稅局遭駭客入侵
- 美國人事管理局遭駭客攻擊
- 歐洲中央銀行網站遭駭

➔ 相關APT事件，在議題二近期駭客攻擊案例分享說明

- 蒐集分析DDoS攻擊事件(2014年~2015年)
 - 歐洲遭遇史上最大DDoS攻擊
 - 蘋果日報台灣與香港網站遭駭客攻擊
 - Evernote、Feedly遭DDoS攻擊
 - Arbor Networks指出2014年上半年DDoS大型攻擊更頻繁
 - GitHub遭遇大規模DDoS攻擊
 - VPN服務Hola遭指控為殭屍網路幫兇
 - 政府機關遭阻斷式服務攻擊日盛
 - 46萬支中國手機發動DDoS洪水攻擊
 - 專門綁架Linux系統的XOR DDoS持續壯大
 - 利用Portmap的DDoS攻擊手法崛起

➔ 相關DDoS事件，第三議題說明

● 蒐集分析惡意程式攻擊事件(2014年~2015年)

- Uroburos間諜程式被揭露
- Darkhotel間諜程式鎖定飯店房客
- WireLurker惡意程式鎖定中國市場蘋果用戶
- 酷派手機植入CoolReaper後門程式
- Lenovo筆電預載Superfish惡意廣告程式
- Equation Group駭客組織開發木馬軍火庫
- Rombertik惡意程式被揭露
- ESET及Kaspersky Lab防毒軟體成為駭客攻擊標的
- Shifu金融木馬程式在日本發動攻擊
- SYNful Knock後門程式鎖定思科(Cisco)路由器攻擊
- TorrentLocker勒索軟體肆虐
- TeslaCrypt勒索軟體鎖定線上遊戲
- Linux.Wifatch路由器病毒自動移除其他惡意程式
- HawkEye後門程式肆虐

沒錢就搗蛋的勒索軟體肆虐

沒錢就搗蛋的勒索軟體肆虐



**最強大勒索軟體
CryptoWall進化到
4.0版，更難偵測，
連檔名都加密！**

CryptoWall 4.0加密的不只是使用者檔案中的資料，甚至還加密了檔案名稱。此舉可讓受



FIGURE 3: Global distribution of CryptoWall 3 ransomware infections

**最壞勒索軟體
CryptoWall 3已造成
3.25億美元損失**

選定CryptoWall進行深入研究的原因包括它是全球最有利可圖也最普及的勒索軟體，去



**Check Point發現
離線執行不需C&C
的勒索軟體**

Check Point深入分析該款勒索軟體後發現，它能夠在不經由C&C伺服器的狀態下加密



**勒索軟體又來了！
這次更本土化**

新變種勒索軟體肆虐，採用更加在地化及客製化的手法，誘使使用者點擊電子郵件中的惡



**臺灣出現NAS勒索
軟體災情，群暉證
實舊版DSM漏洞釀
災**

勒索軟體持續肆虐(1/8)

● 1989年 AIDS Trojan

— 特徵

- 使用者在企圖刪除該惡意程式並重開機90次後，將電腦內的資料夾及檔案進行以對稱式加密技術予以加密

— 散播方式

- 利用磁碟片(Floppy Disk)進行散播

— 勒索方式

- 使用者必須付錢給歹徒指定的帳戶，才能解密再使用



資料來源：<https://www.knowbe4.com/aids-trojan>

勒索軟體持續肆虐(2/8)

● 2013年CryptoLocker

— 特徵

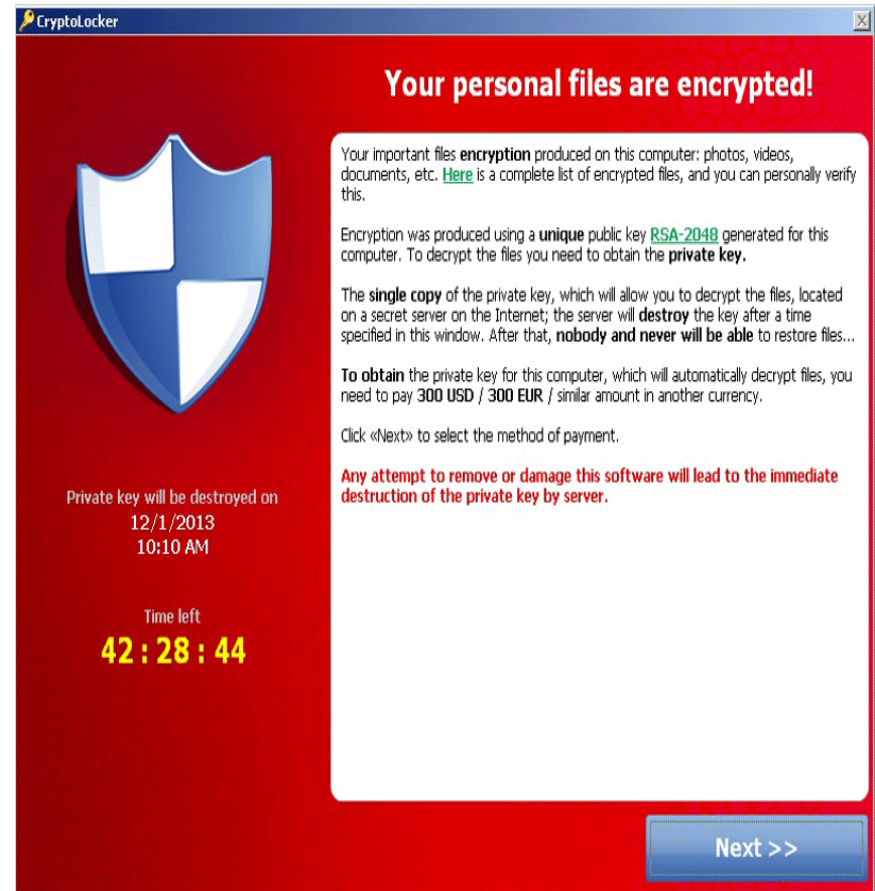
- 更換受害者電腦桌布，並跳出警告訊息，要求在一定期限內，以比特幣(BitCoin)進行付款，否則電腦內被加密的檔案將無法解密

— 散播方式

- 以GameOver Zeus Trojan 之木馬程式傳播

— 勒索方式

- 使用者以比特幣(BitCoin)進行付款，檔案才能解密使用



資料來源：

<http://www.enigmasoftware.com/cryptolockerransomware-removal/>

● 2014年SynoLocker

—特徵

- 登入DSM 管理介面時，顯示資料已經被加密，需要付費才能解密
- CPU 使用率異常地高，或是“synosync” 程序正在運行

—散播方式

- 利用舊版本 DSM 的安全性漏洞

—勒索方式

- 在主網頁面出現勒索訊息，支付約350美元贖金後，才能將NAS硬碟內檔案進行解密復原

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available [here](#).

Follow these simple steps if files recovery is needed:

1. Download and install [Tor Browser](#).
2. Open Tor Browser and visit <http://cyphexfftr7hho.onion>. This link works **only** with the [Tor Browser](#).
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is **19PYBCFK7UoR8PMhhoB8M4gwcPAPXUL3xr** (also visible [here](#)).
5. Follow the instructions on the [decryption page](#) once a valid decryption key has been acquired.

Technical details about the encryption process:

- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwritten with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.

資料來源：<http://www.ithome.com.tw/news/89918>

勒索軟體持續肆虐(4/8)

● 勒索軟體又來了！這次更本土化

- 據iThome報導，新變種勒索軟體肆虐，採用更加在地化及客製化的手法，誘使使用者點擊電子郵件中的惡意連結或執行附加檔案，包括土義英澳日等10多國都傳災情



● 2014年TorrentLocker (fake CryptoLocker)

—特徵

- 依各國語言，客製勒索頁面
- 任意更換受害者的電腦桌布，產生警告訊息，並留下被加密檔案清單
- 不斷與中繼站連線確認受害主機狀態

—散播方式

- 透過社交工程電子郵件中的附檔進行傳播與入侵

—勒索方式

- 以比特幣(BitCoin)進行付款解密

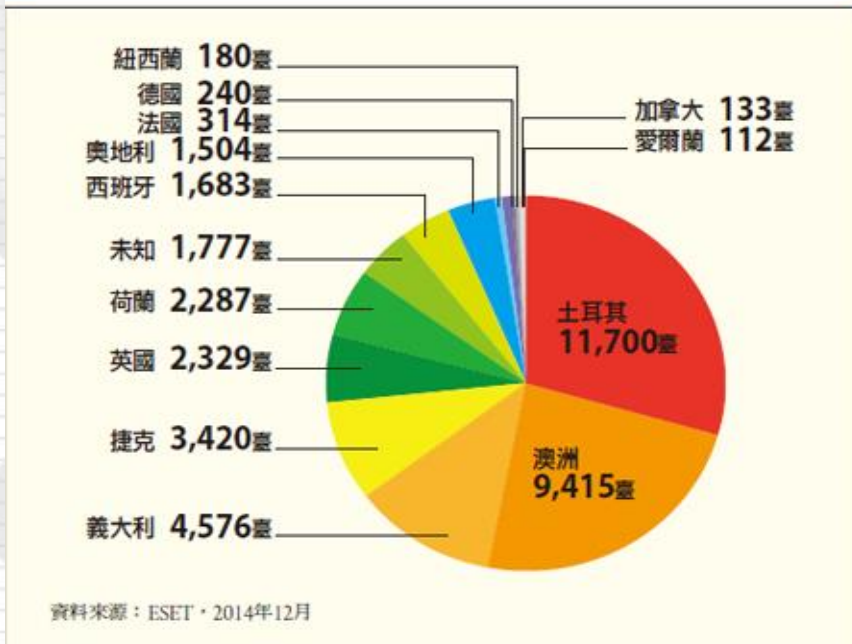


資料來源：<http://botcrawl.com/torrentlocker-virus-removal/>

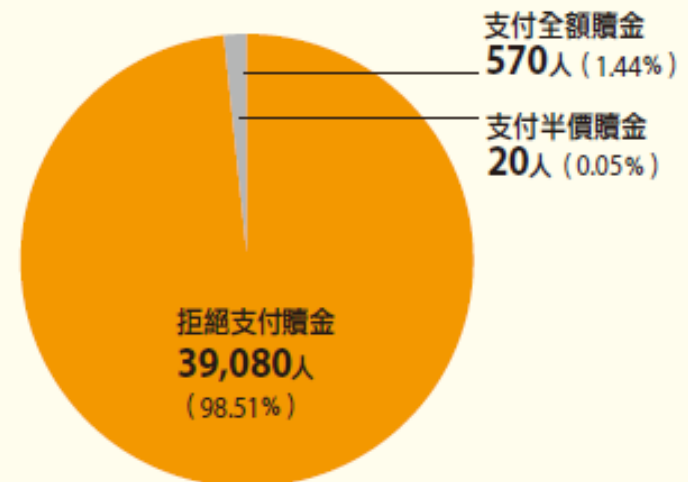
勒索軟體持續肆虐(6/8)

- 依據資安業者ESET統計，感染TorrentLocker主要的地區在歐洲與澳洲，日本也曾發生，但支付贖金比例不到1.5%

TorrentLocker 受駭國家一覽表



支付駭客贖金比例不到1.5%



資料來源：ESET • 2014年12月

● 2014年CryptoWall 3.0

—特徵

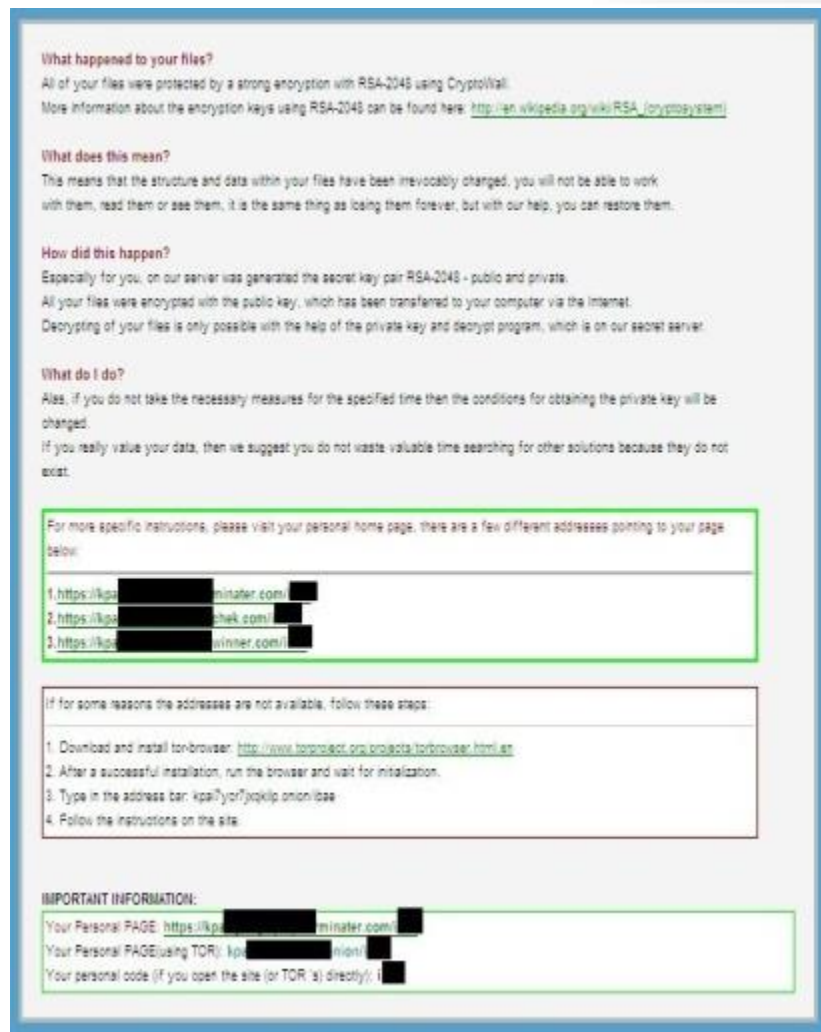
- 依各國語言，客製勒贖頁面
- 任意更換受害者的電腦桌布，產生警告訊息，並留下被加密檔案清單
- 不斷與中繼站連線確認受害主機狀態

—散播方式

- 透過垃圾郵件與偷渡式下載入侵

—勒索方式

- 透過架設於TOR網路的網站以比特幣(BitCoin)進行付款解密



資料來源：

<http://itpro.nikkeibp.co.jp/atclact/active/15/030500023/030500001/?SS=imgviewsuccess&FD=127422348016>

勒索軟體持續肆虐(8/8)

- 依據趨勢科技今年的統計，感染 CryptoWall 3.0 最嚴重的地區為澳洲及紐西蘭，其次是北美和歐洲



資料來源：<http://blog.trendmicro.com.tw/?p=11837>

- 透過社交工程入侵
 - 技術門檻低、效率高、感染範圍易擴散
- 焦點變換到特定目標
 - 企業、政府、特定個人、特定產品.... (目標遭鎖定)
- 使用更進階的閃避技術
 - 利用洋蔥式網路(The Onion Router, Tor)，掩蓋惡意活動和閃躲執法單位，增加犯罪偵查的困難
- 使用虛擬貨幣交易(BitCoin)
 - 交易無法被追蹤，方便洗錢

- 確認電子郵件的寄件者身分
- 仔細檢查郵件內容是否有與事實不符的地方
- 不要開啟來路不明的電子郵件，或點選可疑連結與附檔
- 確保軟體都在最新狀態(作業系統、應用程式及防毒軟體)
- 備份重要資料

衛星導航系統引發國安隱憂

衛星導航系統引發國安隱憂

科技始終來自於人性，好的科技產品為你帶來生活上的便利，但也隱藏危機

- 衛星導航系統，帶你四處趴趴走也不迷路，靠它搞定停車、加油、用餐、住宿或領錢，甚至救援
- 95%以上的太空科技，除了民生用途外，也具有軍事用途，包含：地面作戰部隊的運用、水面艦艇、潛艇的定位與導航、飛彈與戰機的導引
- 中國政府對於衛星導航工業，採取既保守又開放態度，致使中國的衛星導航可能引發一些國安危機

- 全球導航衛星系統(Global Navigation Satellite Systems, GNSS)四大核心供應商
 - 美國全球定位系統(Global Positioning System, GPS)
 - 俄羅斯格洛納斯系統 (GLObal NAvigation Satellite System, GLONASS)
 - 歐盟伽利略定位系統 (Galileo)
 - 大陸北斗衛星導航系統 (Beidou/Compass ,BDS)

- Beidou Satellite Navigation System (BDS) ，中國大陸自主發展、獨立運行的全球衛星導航系統
 - 可與其他系統兼容，用戶可以選擇對自己最有利的系統，得到最佳的服務
 - 衛星定位終端與衛星或地面服務站間，進行簡訊通報，**具雙向的訊息傳遞**，GPS僅能單向通報
 - 以軍事使用為主，可全天候、任何地點、任何時間、不限人數來進行使用
 - 北斗衛星導航系統提供定位、導航、授時服務，分為開放服務和授權服務兩種方式

- 授權用戶

- 提供更安全與更高精度的定位、測速、授時、資訊收發服務(軍用版容量為120個漢字，民用版49個漢字)以及系統完好性資訊

- 開放服務

- 免費提供定位、測速、授時服務，定位精度10米，測速精度0.2米/秒，授時精度10ns

- 系統架構

- 採用主動型雙星定位系統，定位終端為兼具接收與發送的「有源定位」
- 定位與速度解算需經過地面中心，終端需先註冊使用權限

- 應用領域

- 水利電力、海洋漁業、交通運輸、國土測量、救災與公共安全等領域，不利於軍事用途

- 現況

- 衛星的壽命到期後（設計值8年），系統已停止工作

- 系統架構

- 太空部份 (Space Segment)

- 由5顆靜止軌道衛星和30顆非靜止軌道衛星組成

- 地面控制部份 (Control Segment)

- 建置若干地面站包括主控站、注入站和監測站

- 用戶端部份 (User Segment)

- 配備衛星訊號接收器的用戶、與其他衛星導航系統相容的終端設備

- 採用無源定位，與GPS系統相似，並與北斗一號兼容

- 應用領域

- 同北斗一號，增加軍事用途

- 現況

- 持續針對民生與軍事用途進行發展

● 北斗一號

- 用戶需進行註冊，有個資外洩的疑慮
- 定位與速度解算需經過地面控制中心，可能會被監控定位
- 具雙向資訊收發功能，可向指定用戶的GPS程式發送隱藏指令(e.g.竊聽、竊取資料、發起網路攻擊...)
- 定位晶片均為中國製品，可能會被藏有惡意功能

● 北斗二號

- 具雙向資訊收發功能，可向指定用戶的GPS程式發送隱藏指令，取得特定個人資訊後，即可針對特定人士進行監控定位

- 公務人員不應向北斗系統進行使用者註冊
- 不購買支援北斗衛星導航系統的產品
- 個人使用設備，應減少保存個人資料於該產品中
- 國安相關單位，應建立北斗衛星導航系統監聽機制，監看中國透過衛星訊號進行入侵攻擊情勢
- 必要時建置電子干擾器予以反制

NFC卡便捷但個資要留意



NFC卡便捷但個資要留意

- 智慧IC卡

- 台胞證...

- 申請自助通關備案後，可自助通關
 - 免加簽節省費用

E化後的台胞證，從入關到住宿，資訊是否全都露？

- 行動支付

- 快速完成交易

- 結合信用卡(小額付費、感應式付款)

- 智慧型手機成為最好的NFC功能載具

- 整合多張卡片
 - 手機隨身攜帶

NFC 手機信用卡來了，但安全性夠嗎？

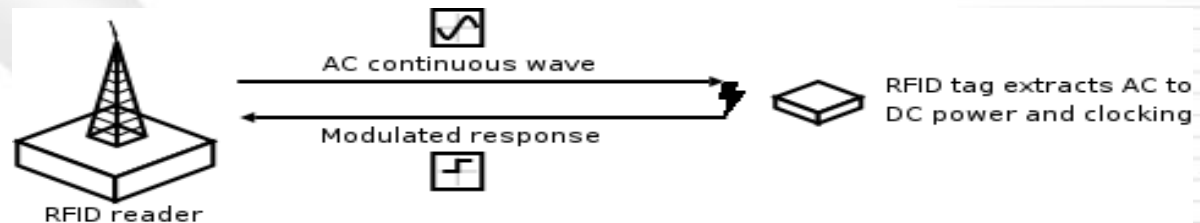
近距離無線通訊(NFC)

- 近距離無線通訊，是一種短距離的高頻無線通訊技術
- 允許電子裝置之間進行非接觸式點對點資料傳輸，在十公分內交換資料
- NFC技術由非接觸式射頻識別（RFID）演變而來，其基礎是RFID及互連技術

無線射頻辨識(Radio Frequency Identification, RFID)，一種無線通訊技術，透過無線電訊號識別特定的目標與數據

● 被動式

- 沒有內部供電電源，藉由讀取器發射出的電磁波獲得能量，並回傳相對應的反向散射訊號至讀取器



● 半被動式

- 運作原理同上，多了一顆小型電池，增加回傳訊號的功率

● 主動式

- 標籤本身具有內部電源供應器，主動發射內部標籤的記憶體資料到讀取器上

● Type B (ISO/IEC 14443 Type B) 國際標準

- “Tag Information”
- 紀錄Type B標準所定義的參數

● ISO/IEC 7816-4 國際標準

- “epassport (MRTD)”
- 紀錄卡式台胞證持卡人的資訊

	ISO 14443B
感應距離	數十公分至數公尺
編碼方式	◆ PCD to PICC: 位元編碼方式為NRZ Code；信號調變方式為ASK 10% 信號 ◆ PICC to PCD: 位元編碼方式為NRZ Code；信號調變方式為BPSK調變。
通信速度	106KBps
提倡者	Motorola(美國), NEC
用途	遠距離
例子	1. 貨櫃、貨箱盤點 2. 居民基本資料卡

資料來源：https://zh.wikipedia.org/wiki/ISO/IEC_14443

http://www.iso.org/iso/catalogue_detail.htm?csnumber=54550

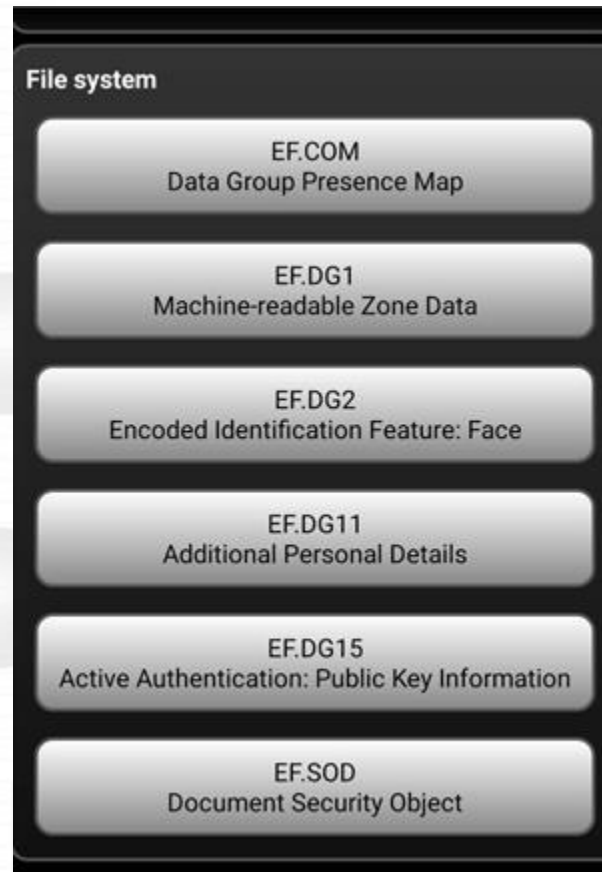
http://staffweb.ncnu.edu.tw/hychien/course/RFID_introduction.pdf

卡式台胞證之資安疑慮

- 使用支援NFC Tag 之Reader讀取卡片資料
 - NFC是一種短距高頻的無線電技術，在13.56MHz頻率運行於20公分距離內



資料來源：<https://zh.wikipedia.org/wiki/%E8%BF%91%E5%A0%B4%E9%80%9A%E8%A8%8A>
https://play.google.com/store/apps/details?id=at.mroland.android.apps.nfctaginfo&hl=zh_TW



台胞證上的資訊

證件照片

附加資訊

存放公鑰

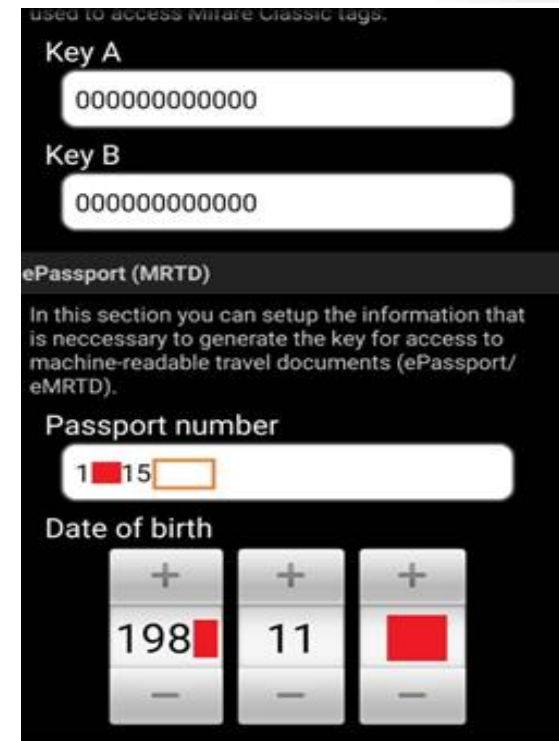
記錄發證單位與證件用途

解密流程1-輸入基本資訊

- 有關ISO/IEC 7816-4 電子識別卡(ePassport)資安防護國際標準，這部分解密需先輸入以下資料進行驗證：

- Access Key(Key A、Key B)
- 台胞證號碼(Passport Number)
- 西元出生年月日
- 台胞證到期日

註: Access Key為類似一組存取卡片的帳密



used to access Mifare Classic tags.

Key A
000000000000

Key B
000000000000

ePassport (MRTD)

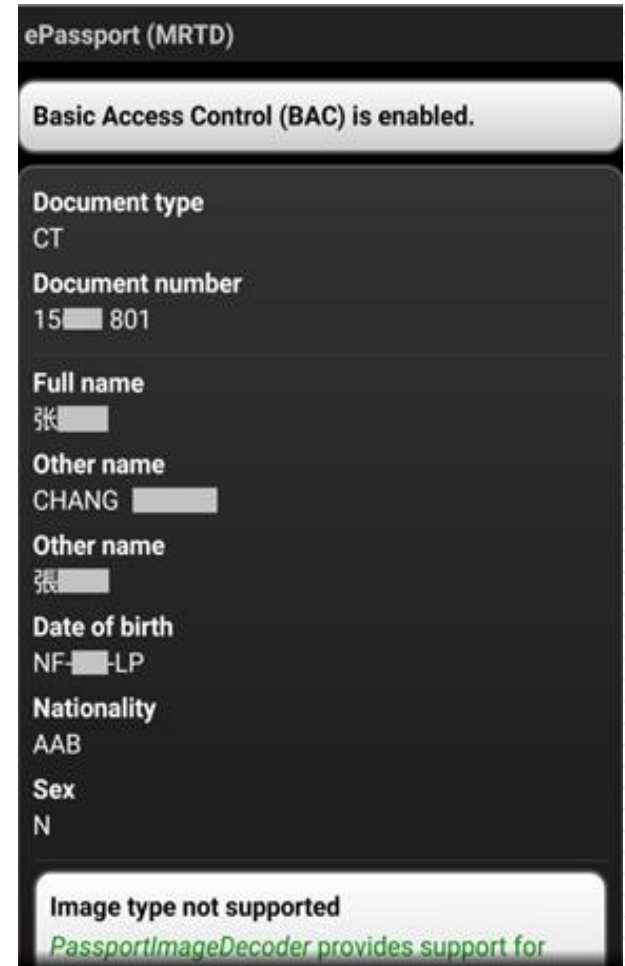
In this section you can setup the information that is necessary to generate the key for access to machine-readable travel documents (ePassport/eMRTD).

Passport number
1 15

Date of birth
198 11

解密流程2-取得卡片上資訊

- 輸入前述資訊後，若驗證成功，即可取得台胞證(ePassport)上資訊，其包含：
 - 台胞證類別(旅遊/公務/其他)
 - 姓名(簡體/繁體/英文)
 - 出生年月日
 - 國籍
 - 性別



卡式台胞證之資安疑慮

- 卡式台胞證係參照國際民航組織DOC9303 TD-1之標準製作，可透過資訊系統自動讀取
- 採用被動式無線射頻辨識(RFID)技術
- 本身並無發射訊號能力，不具衛星定位功能
- 晶片容量未逾0.1MB，未包含指紋等生物特徵資料

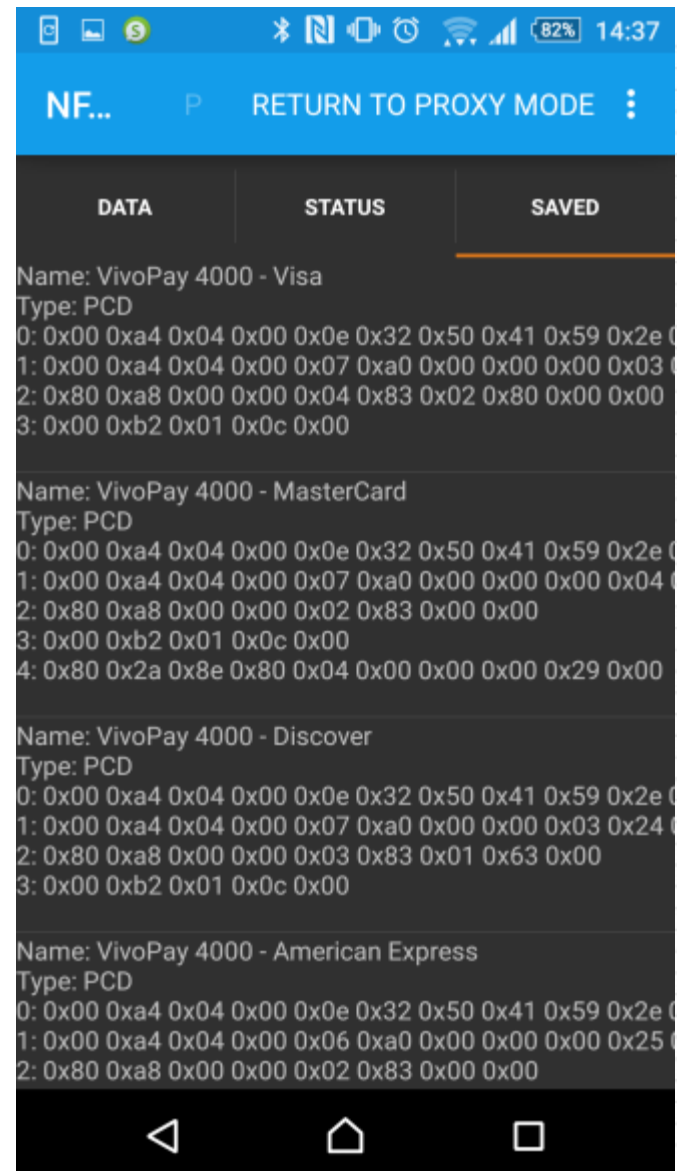
防止資訊外洩建議

RFID標籤無須直接與收發器接觸，使用者會在不知情的情況下被他人讀取標籤內存儲的資訊，構成安全隱憂

- 阻絕卡片追蹤與定位功能
 - 可考量全程採用RFID 屏蔽(blocking)錢包，以避免被掃描定位與辨識
- 持續關注隱私資訊儲存情形
 - 持續掌握相關資料蒐集與卡式台胞證之關聯性，即早因應隱私資料外洩或遭濫用之資安風險
- 公務人員或涉密人員前往中國應依法申報

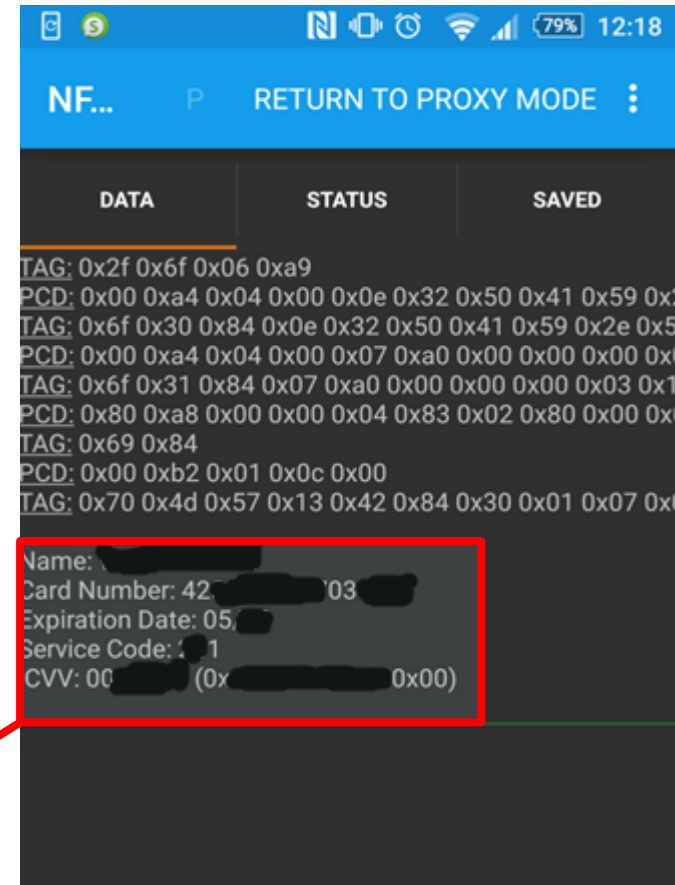
NFC信用卡之資安疑慮

- 模擬 POS 型號
 - 工具：NFCProxy
 - 型號：VivoPay 4000



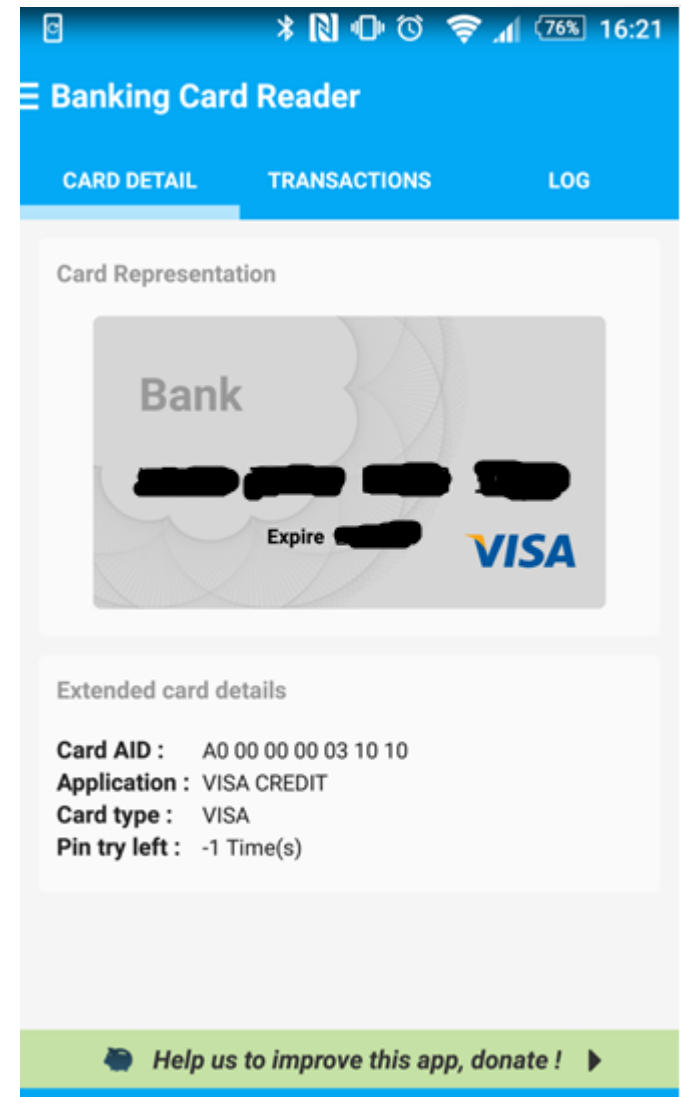
● 可被讀取資訊

- 姓名
- 卡號
- 卡片過期日
- 服務碼 (Service Code)
- 晶片卡驗證值 (iCVV, Integrated Chip Card Verification Value)



發卡銀行產生安全認證碼之資訊

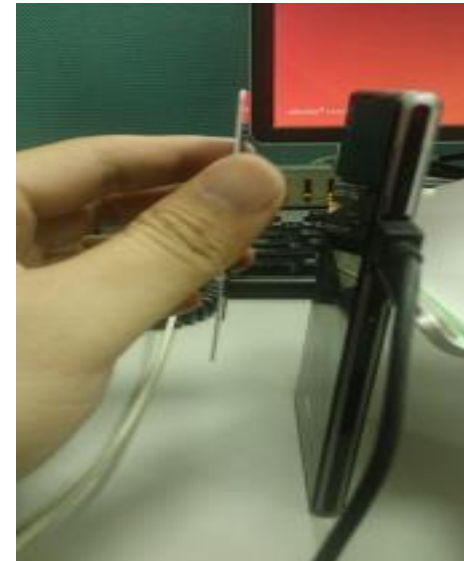
- Bank Card Reader 讀取資訊
 - 信用卡號碼
 - 卡片類別
 - 交易紀錄 (因採模擬方式測試，無法擷取交易資訊)



- 實際測試結果

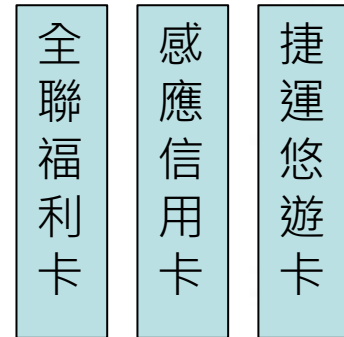
- 感應式信用卡與讀卡機距離 **4 到 5** 公分，即可被讀卡機讀取。

- 若將感應式信用卡放入錢包中，錢包內無其他卡片，則信用卡與讀卡機距離約 **3 到 4** 公分，即可被讀取。



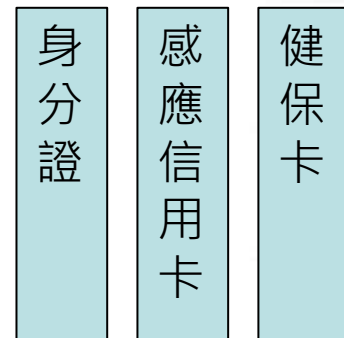
● 實際測試結果

–如左(圖一)所示，將感應式信用卡置中，前後分別置有 RFID 線圈卡片，如全聯福利卡與捷運悠遊卡。實驗結果，讀卡機**無法**讀取信用卡資訊。



圖一

–如左(圖二)所示，將感應式信用卡置中，前後分別放置無 RFID 線圈卡片，如身分證與健保卡。則讀卡機。實驗結果，讀卡機**可**讀取信用卡資訊。



圖二

信用卡 \ 讀卡機 APP	Banking Card Reader	NFCProxy
國泰世華 Costco 聯名卡	可	可
國泰世華 Play 悠遊聯名卡	可	不可
中國信託信用卡	可	不可
玉山悠遊聯名卡	可	不可
台新新光三越聯名卡	可	不可

- 措施一

- 建議只安裝 Google Play 或 Apple App Store 上之應用程式，避免安裝從地下論壇或其他來源之應用程式

- 措施二

- 以非接觸方式讀取的資料，只限於必須用來交易的資料，且不能包括用戶全名

- 措施三

- 使用感應式信用卡付費時，建議增加其他驗證機制。例如：讓持卡人自行輸入交易密碼

- 措施四

- 提供刷卡消費簡訊或e-mail通知，提供消費者告知與確認交易紀錄

結論與建議

- 避免購買支援北斗衛星導航系統的產品，國安相關單位，應建立監聽與干擾機制
- 有關非接觸式(感應式) IC智慧卡，建議採用RFID屏蔽(blocking)錢包，以避免被掃描定位與辨識
- 養成良好的郵件使用與資料備份習慣，減少被勒索軟體威脅的機會

報告完畢
敬請指教