資安威脅趨勢與案例分享

行政院國家資通安全會報技術服務中心

108年12月

大綱

- 資安威脅趨勢
  - **資安攻擊活動分析**
- 資安威脅案例
  - PWSH威脅案例
  - 電子郵件受監看案例
  - 智慧手機詐騙利用案例
- 結論與建議

本年政府機關資安威脅情勢

01

資料外洩事件仍頻

資料外洩管道有轉移至社群網站趨勢，影響範圍廣大

02

供應鏈攻擊持續發生

- 駭客藉由入侵特定軟/韌體開發公司或人員電腦，進行竄改程式或下載連結等行為，造成大範圍的感染與擴散
- 最大特色是利用受信任的管道進行散播
- 入侵軟體開發廠商後，可以其做為跳板，滲透客戶組織

03

APT類型攻擊轉向透過網頁漏洞進行入侵

網頁攻擊多透過偵查搜尋，鎖定未更新或存在漏洞主機做為攻擊目標，建議機關應強化漏洞更新修補與管理機制

04

物聯網攻擊持續鎖定網通設備

持續鎖定網通設備做為攻擊標的，並研發功能完整的控制程式，未來將有更精巧地詐騙手法

108年資安事件關聯綜覽

108/3

20家政府機關、國營企業與金融單位存在公文附件未公開下載系統漏洞，駭客利用此漏洞入侵部分機關植入網頁型後門

SPEED™ 公文檔案附件下載系統

108/3-108/7

駭客入侵機關網站並使用中國蟻劍後門管理工具，共計入侵24個機關

108/5

微軟RDP漏洞(CVE-2019-0708)，發現 44個機關暴露於網際網路受影響

108/3-108/7

108/8-108/9

資安研究人員公布VPN重大漏洞
共計11間機關VPN漏洞可遭利用

Pulse Secure

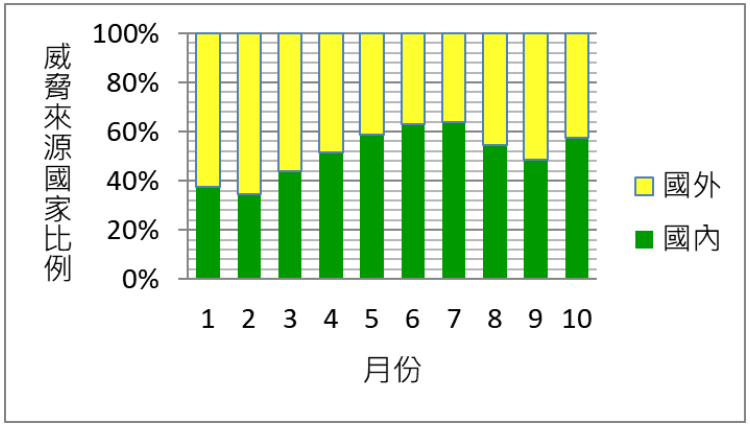
108/09

駭客使用DNS Tunnel進行受害主機控制與連線，影響10家

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

108年政府機關資安聯防監控統計

- 108年1月1日至10月31日，SOC業者回傳之有效事件單數量共155,382件
  - 依資安威脅種類排名前3名分別為入侵攻擊類(40%)、掃描刺探類(33%)及惡意程式類(15%)
  - 依政府機關業務類別排名前3名分別為綜合行政類(39%)、經濟能源農業類(20%)及內政衛福勞動類(14%)
- 國外攻擊來源
  - 美國(40%)
  - 中國(8%)
  - 加拿大(5%)
  - 其他攻擊來源國家眾多共151國



資安聯防監控威脅類型統計(1/2)

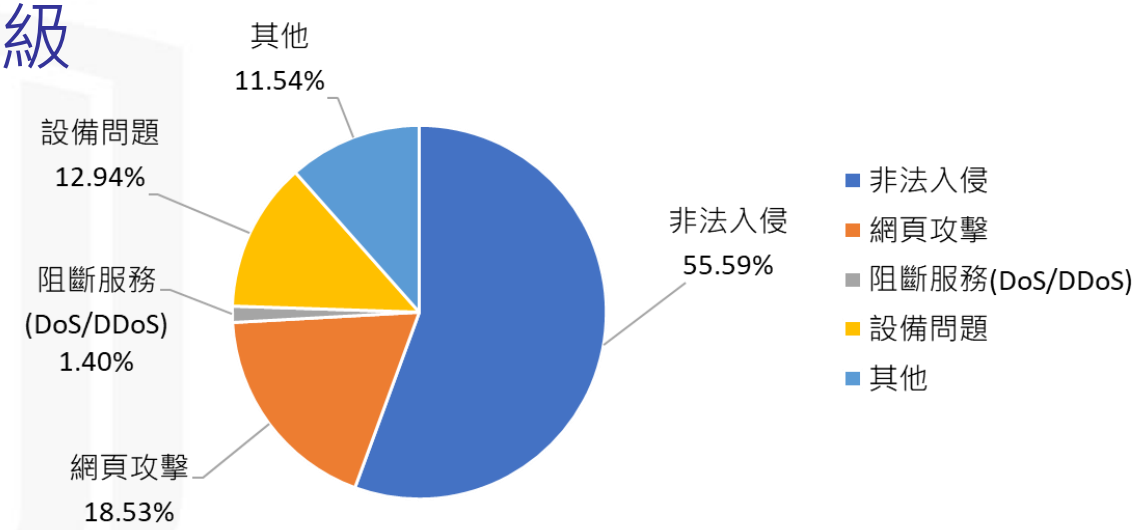
- 國外攻擊來源國家的監控事件
  - 外部主機執行大規模弱點掃描攻擊
  - 弱點與漏洞利用
  - 垃圾郵件SPAM
  - 網頁入侵行為
  - 外部主機嘗試SQL-Injection攻擊
- 國內來源的監控事件
  - 弱點與漏洞利用
  - 後門間諜行為
  - 網頁入侵攻擊
  - 內部主機疑似進行大量網路芳鄰連線
  - 內部主機單次連線至惡意IP
  - 內部主機疑似進行P2P連線

資安聯防監控威脅類型統計(2/2)

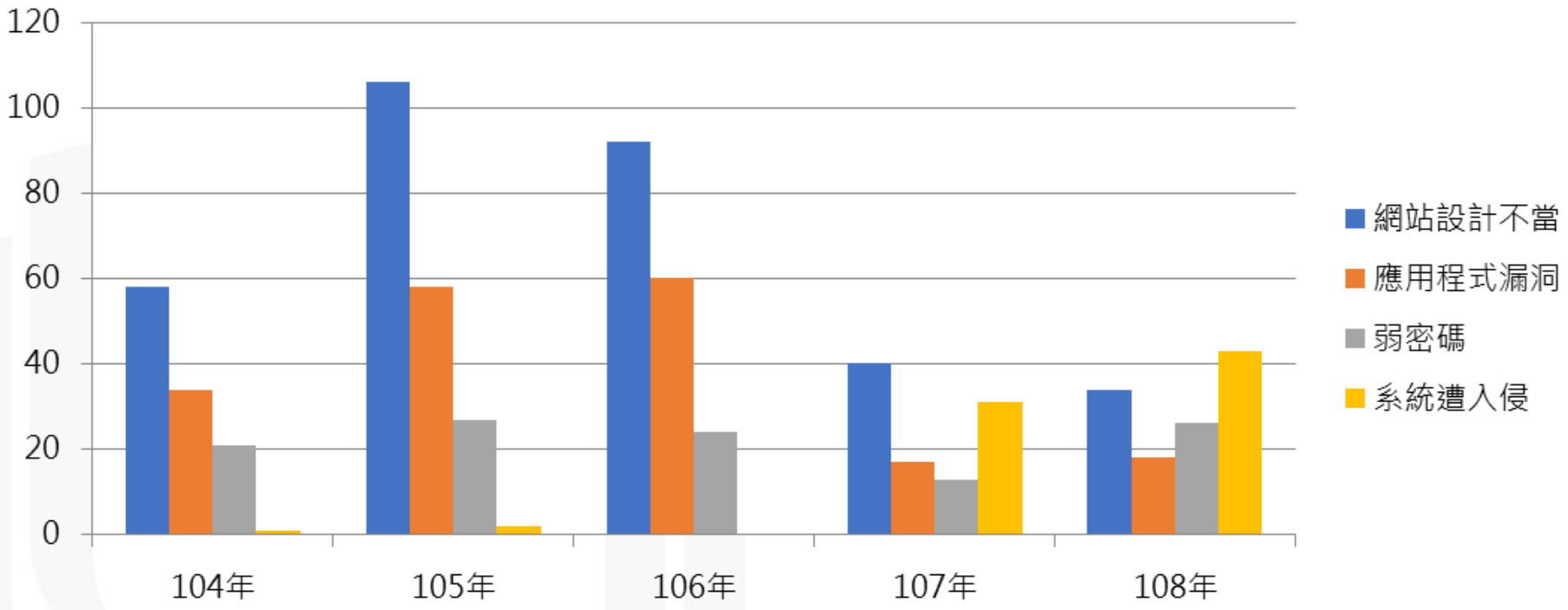
- 中國來源的監控事件
  - 發現網頁攻擊事件
  - 密碼猜測行為
  - 遠端存取控制行為

108年政府機關資安事件通報統計

- 108年1月1日至11月30日共接獲286件資安事件通報，其中52.80%(151件)為各機關接獲技服中心警訊通告後所進行之通報
- 通報資安事件等級
  - 4級事件：0件
  - 3級事件：11件
  - 2級事件：42件
  - 1級事件：233件



政府機關資安事件主要發生原因



註：108年資料統計至11月30日

政府機關重大資安事件通報統計

108年接獲11件政府機關重大資安事件通報
8件為資料外洩
3件為核心業務中斷

資料外洩發生原因

- 網站設計不當，遭駭客利用網站漏洞存取敏感資料
- 機關內部遭駭客潛伏非法入侵，竊取敏感資料
- 機關內部人員疏失，造成敏感資料公開於網際網路存取

核心業務中斷發生原因

- 機關遭非法入侵植入勒索軟體，因無法啟用備援機制，影響核心業務運作
- 變更管理失當，造成伺服器服務能量失衡，影響核心業務運作
- 設備故障，影響涉及關鍵基礎設施維運之核心資通系統運作

註：108年資料統計至11月30日

重大通報個資外洩案例一

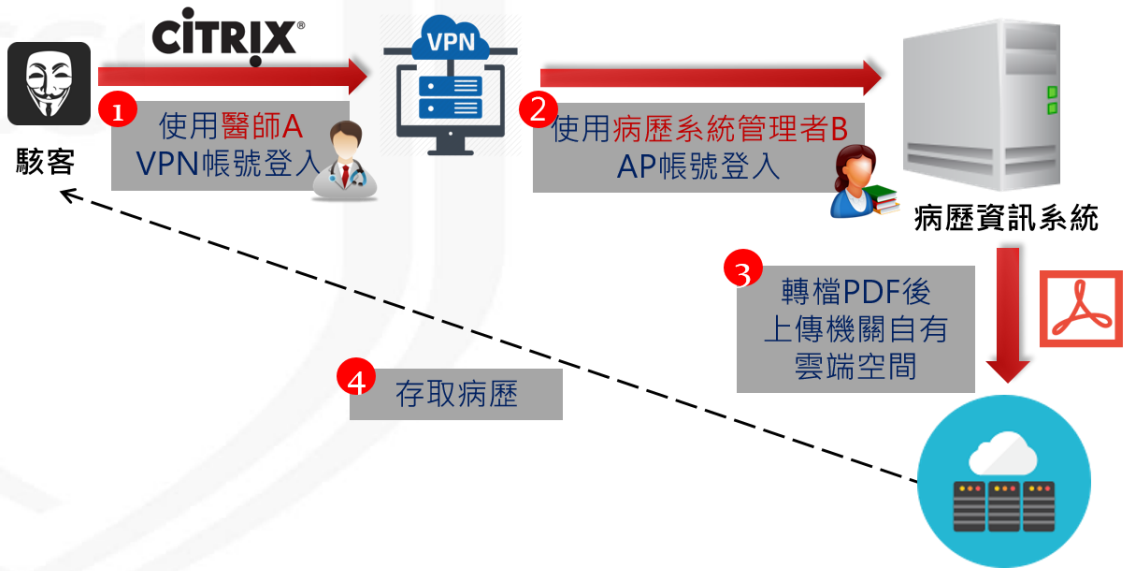
案情提要

- 國外Raidforums論壇刊登疑似OO部掌管之公務人員資料，內容包含軍公教人員之姓名、身分證字號、服務單位及職務等個人資料
- 透過技術檢測及實地查核發現，OO部內外重要資通系統之日誌或稽核紀錄保存不完整、核心系統發現若干應用程式存在高風險弱點，並高度仰賴委外廠商，且第三方檢測機制未能有效協助機關發掘潛在威脅

重大通報個資外洩案例二

案情提要

- 本年9月間某醫院進行資安內部查核時，發現異常連線，經查係駭客盜用內部人員帳號登入VPN並存取病歷資訊系統
- 該醫院於發現異常時，即請使用者立即更換密碼，惟並未具強制性，導致後續持續發生帳號遭盜用情事



重大通報個資外洩案例三

案情提要

- 駭客入侵醫療院所資訊服務廠商，並透過健保VPN將勒索病毒感染至醫療院所，導致醫療院所電腦無法正常運作，惟未造成資料外洩
- 透過實地查核發現，健保VPN管理機制待加強，VPN內部未設置存取控管機制，且目前針對資訊服務業者之資安防護未有要求，亦未限制資訊服務業者連線範圍

大綱

- 資安威脅趨勢
  - 資安攻擊活動分析
- 資安威脅案例
  - **PWSH威脅案例**
  - 電子郵件受監看案例
  - 智慧手機詐騙利用案例
- 結論與建議

案例說明

- 技服中心透過惡意電子郵件檢測機制，發現使用PowerShell(PWSH) 之電子郵件社交工程攻擊手法有增加趨勢
- 108年1月至5月總計蒐集2,060個含有PWSH攻擊手法之社交工程惡意文件，並從中發現採用「退信攻擊」之社交工程信件
- 駭客透過PWSH蒐集主機資訊後，回報至Gmail郵件信箱，並將惡意PWSH檔案放置於Dropbox雲端空間，藉此躲避網路偵測機制與提高成功率

PWSH惡意行為分類

項次	行為類別	說明
1	啟動PowerShell	以系統程式帶起PowerShell，以執行相關腳本指令，常見系統程式如： CMD、PowerShell及WMIC等
2	隱匿執行	用來隱藏PowerShell執行或互動視窗，常見指令/參數如：-WindowStyle Hidden, -W Hidden、-NonInteractive、-NonI、-NoLogo等
3	繞過執行限制政策	繞過系統對PowerShell腳本執行的限制，使駭客能輕易透過腳本對系統進行操作，常見指令/參數如：-ExecutionPolicy Bypass、-Exec Bypass、Set-ExecutionPolicy Unrestricted等
4	指令/腳本混淆	以混淆手法來隱藏惡意指令代碼，藉此迴避特徵比對偵測。混淆手法包括： 大小寫混雜、單雙引號混用、斷字聯結、插入空白或無用字元、字串變位、ASCII/Hex編碼、Base64編碼、Secure key加密、字串疊代等
5	腳本解碼	針對已混淆的PowerShell腳本進行解碼並執行
6	下載程式	進行下載行為，通常透過PowerShell指令至特定網站下載檔案，或於下載後直接於記憶體中執行，常見指令/參數如：New-Object System.Net.WebClient).DownloadString()、New-Object System.Net.WebClient).DownloadFile()等
7	執行程序	於目標系統安裝套件與工具，常見指令/參數如： Start-Process、Invoke-Expression、New-Service、ShellExecute等

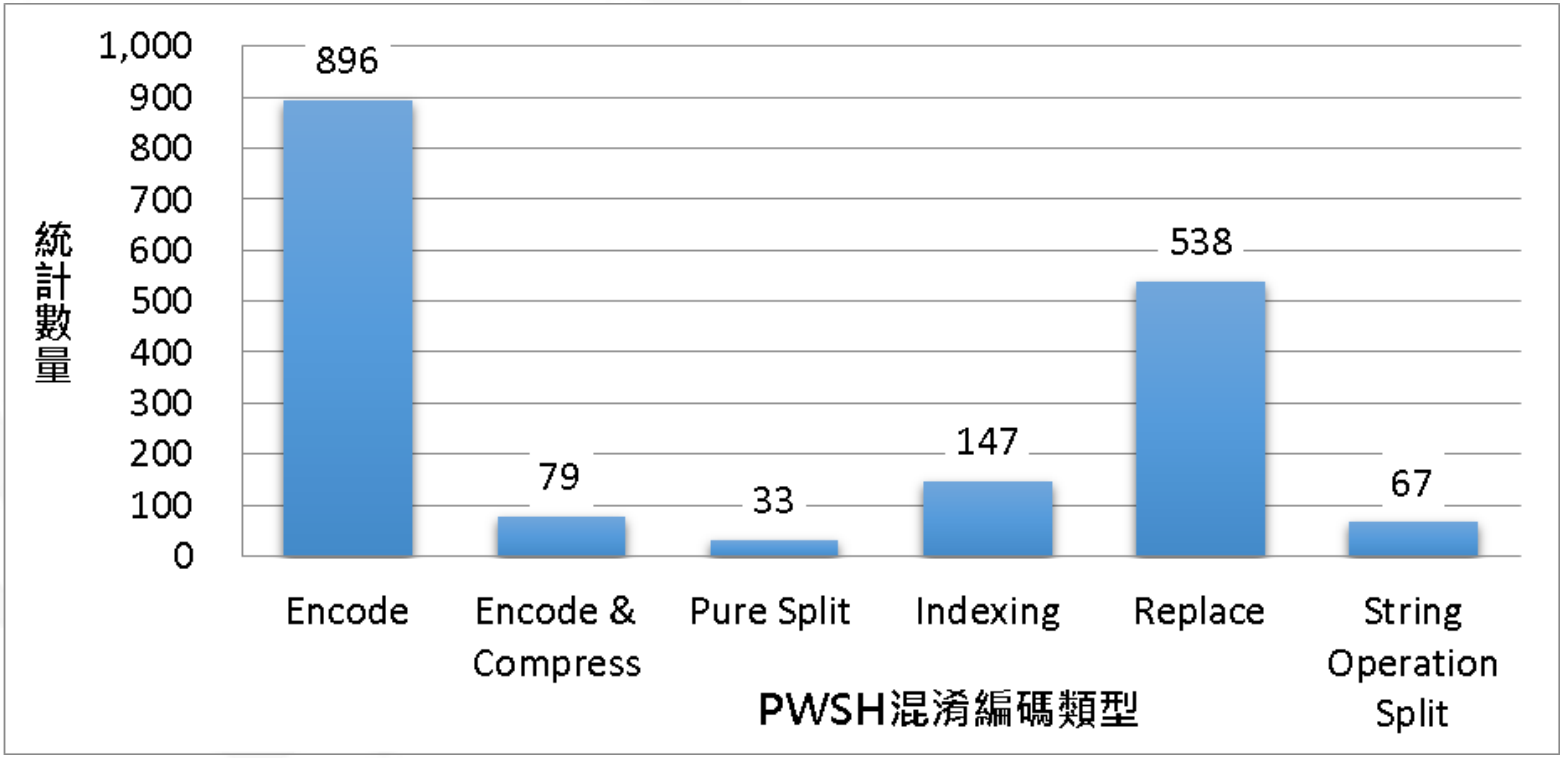
PWSH混淆類型分析

- 分析PWSH惡意腳本，可將混淆機制大致分成6種類型

項次	編碼類別	說明
1	編碼 (Encode)	以Base64進行混淆編碼之手法
2	編碼與壓縮 (Encode ＆ Compress)	以Base64進行混淆編碼後，再將其字串壓縮之混淆手法
3	純切割 (Pure split)	使用特定字元或字串穿插在整體系統指令字串中，達到混淆之目的
4	索引取代 (Indexing)	在整體系統指令字串中，放置一段索引表及亂數字串，透過索引值去對照亂數字串的個別字元位置後取代字元進行混淆
5	字串取代 (Replace)	執行系統指令前使用Replace函式取代特定參數使惡意PowerShell可正常執行之混淆手法
6	任意字元穿插 (String operation split)	用多種字元重複穿插在字串其中，達到混淆之目的

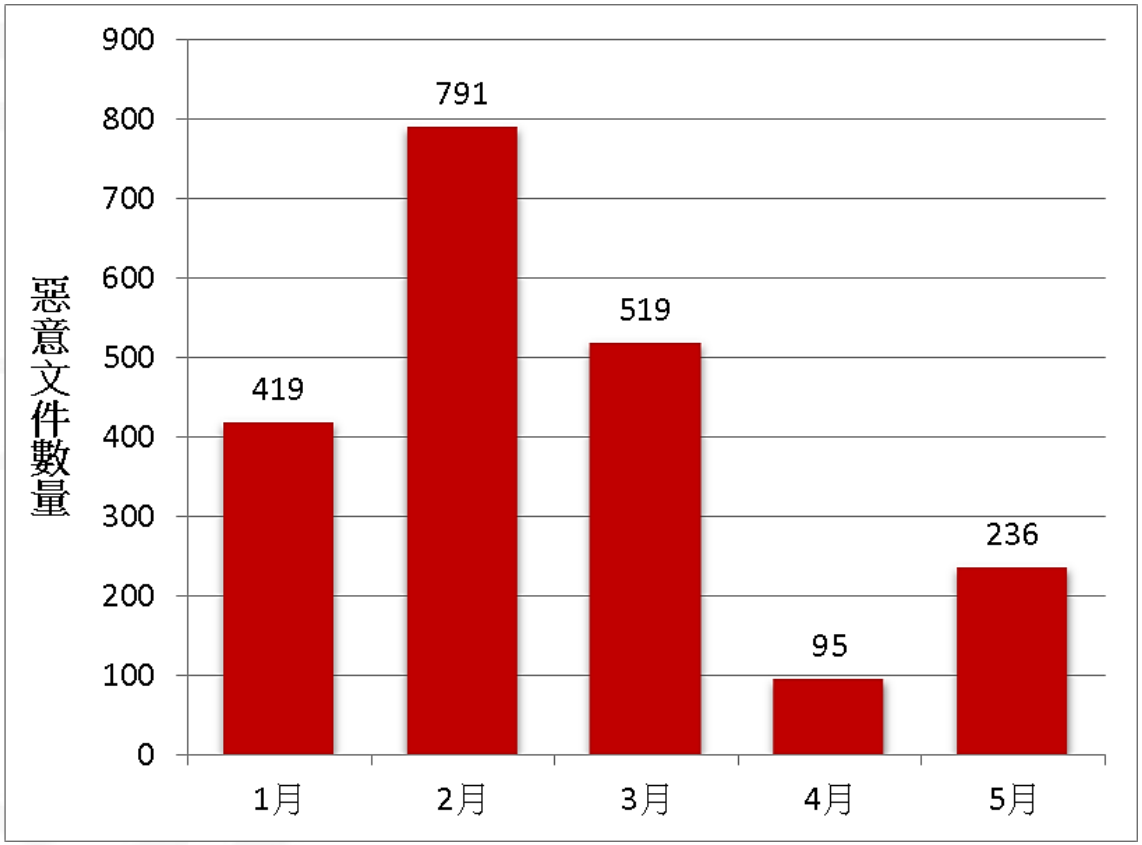
PWSH混淆類型統計

- PWSH惡意腳本中，前3名混淆機制分別為：編碼(Encode)、字串取代(Replace)及索引取代(Indexing)
  - 部分混淆無法解析或無法正常執行之腳本則不列入統計



PWSH威脅趨勢統計

- 108年1月至5月總計蒐集2,060個含有PWSH攻擊手法之社交工程惡意文件

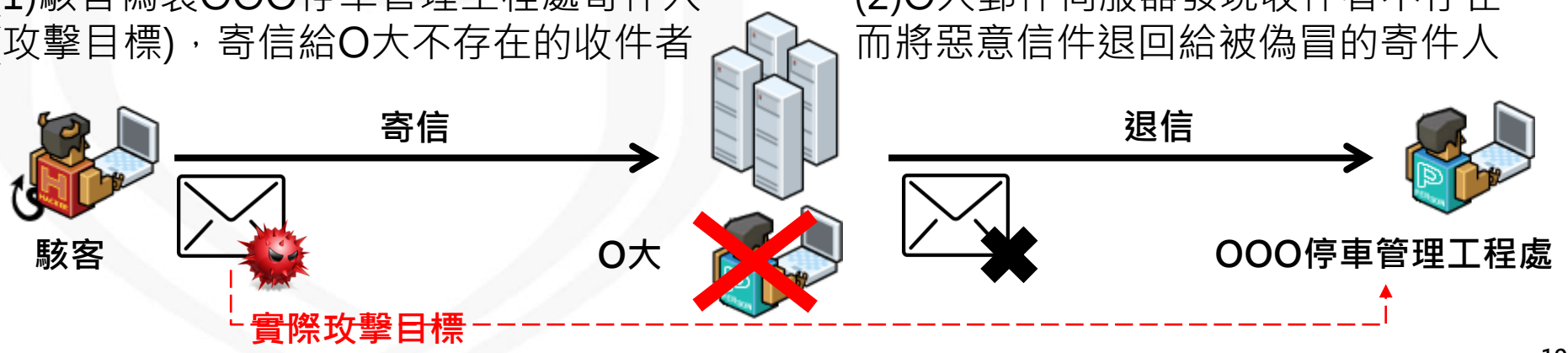


PWSH社交工程案例分析(1/2)

- 技服中心於108年5月發現駭客偽冒OOO停車管理工程處，透過寄送惡意電子郵件至OO大學郵件伺服器，以帳號不存在被伺服器退信的方式，繞過電子郵件中的寄件者政策架構(Sender Policy Framework, SPF)驗證機制，藉此攻擊OOO停車管理工程處，該攻擊方式亦稱為「退信攻擊」

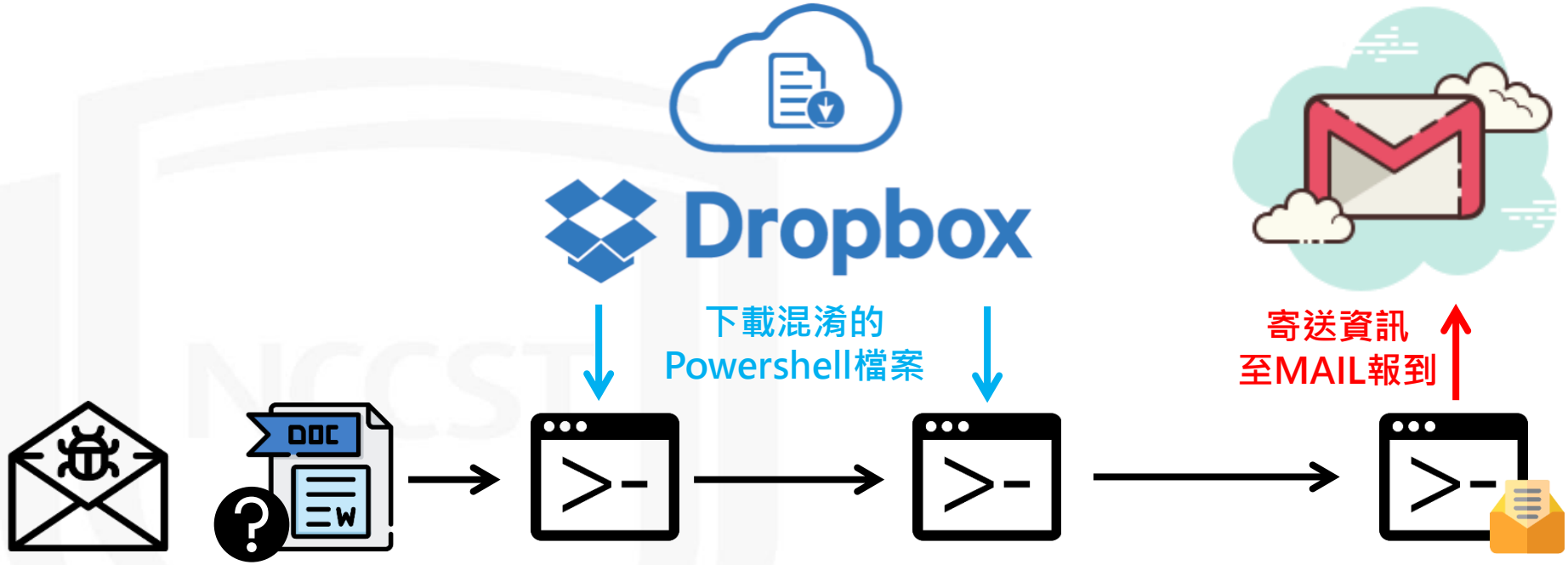
(1)駭客偽裝OOO停車管理工程處寄件人(攻擊目標)，寄信給O大不存在的收件者

(2)O大郵件伺服器發現收件者不存在，而將惡意信件退回給被偽冒的寄件人



PWSH社交工程案例分析(2/2)

- 經取得駭客所使用的惡意PWSH與分析攻擊手法，綜整此PWSH無檔案威脅攻擊運作流程如下



1. 使用者點擊惡意附檔確認是否寄錯檔案，惡意文件透過巨集執行1階惡意PWSH
2. 1階惡意PWSH連線至Dropbox下載並執行2階惡意PWSH
3. 2階惡意PWSH再次連線至Dropbox下載並執行3階惡意PWSH，設定開機再次下載2階惡意PWSH
4. 2階惡意PWSH完成持續性運作設定後，執行系統指令將主機資訊寄回信箱

大綱

- 資安威脅趨勢
  - 資安攻擊活動分析
- **資安威脅案例**
  - PWSH威脅案例
  - **電子郵件受監控案例**
  - 智慧手機詐騙利用案例
- 結論與建議

報紙紕漏(1/2)

中山大學驚傳師生電子郵件被監控長達3年，起因是駭客濫用Open WebMail漏洞，其他學校也應留意相關系統安全

採用Open WebMail建置電子郵件系統的單位要注意了！最近中山大學坦承，他們的電子郵件信箱遭到入侵逾3年，駭客監控近百人的信件，其中大部分是社會學系的教授

文/ 周峻佑 | 2019-11-08 發表

讚 5.8 萬 按讚加入iThome粉絲團 讚 491 分享

圖片來源: 中山大學

首頁 / 重點新聞

獨家／中山大學逾10位兩岸研究學者 電郵疑遭駭3年

最新更新：2019/11/08 01:37

報紙紕漏(2/2)

- ...媒體報導，從2016年下半年起，有身分不明的人士，利用Open Webmail系統漏洞，創設數個假帳號，冒充校方資深行政人員，監看10多位教授的電子郵件信箱內容，監看對象包括政治學研究所、亞太所與政經系教授。入侵者的網際網路協定位址（IP位址）有從美國、中國、香港登入紀錄，自今年以來集中出現於香港網域，高度懷疑是使用虛擬私人網路（VPN）產生的網域地址...

大綱

- 資安威脅趨勢
  - 資安攻擊活動分析
- 資安威脅案例
  - PWSH威脅案例
  - 電子郵件受監看案例
  - **智慧手機詐騙利用案例**
- 結論與建議

案例說明

- 駭客利用台灣IP建立惡意APK下載站偽裝成Google Play商店APP下載頁，APP偽冒對象為韓國行政安全部警察廳的手機反間諜服務、韓國各家金控業者的信用貸款服務及韓國資安業者BTWorks的防釣魚軟體

警察廳反間軟體

偽冒的惡意APK下載站

現代汽車

新韓銀行

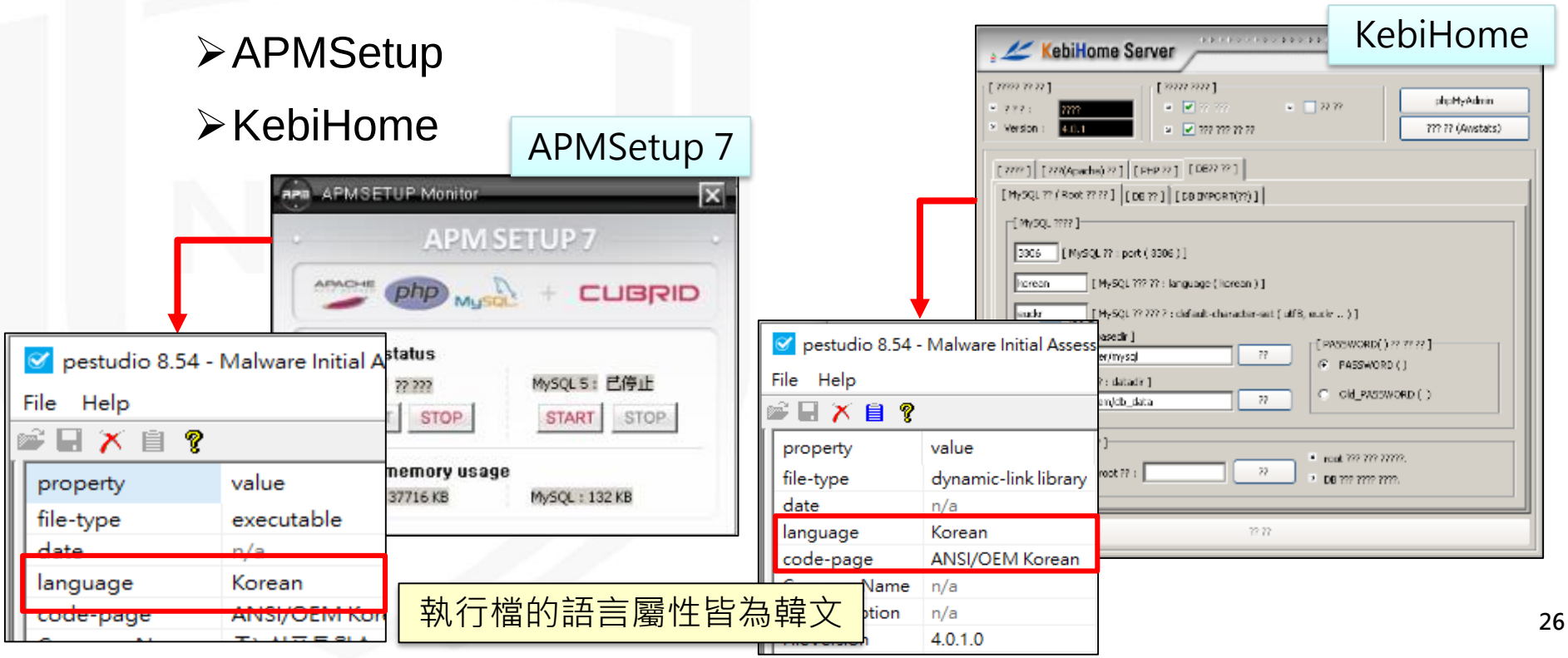
南韓韓亞銀行

南韓國民銀行

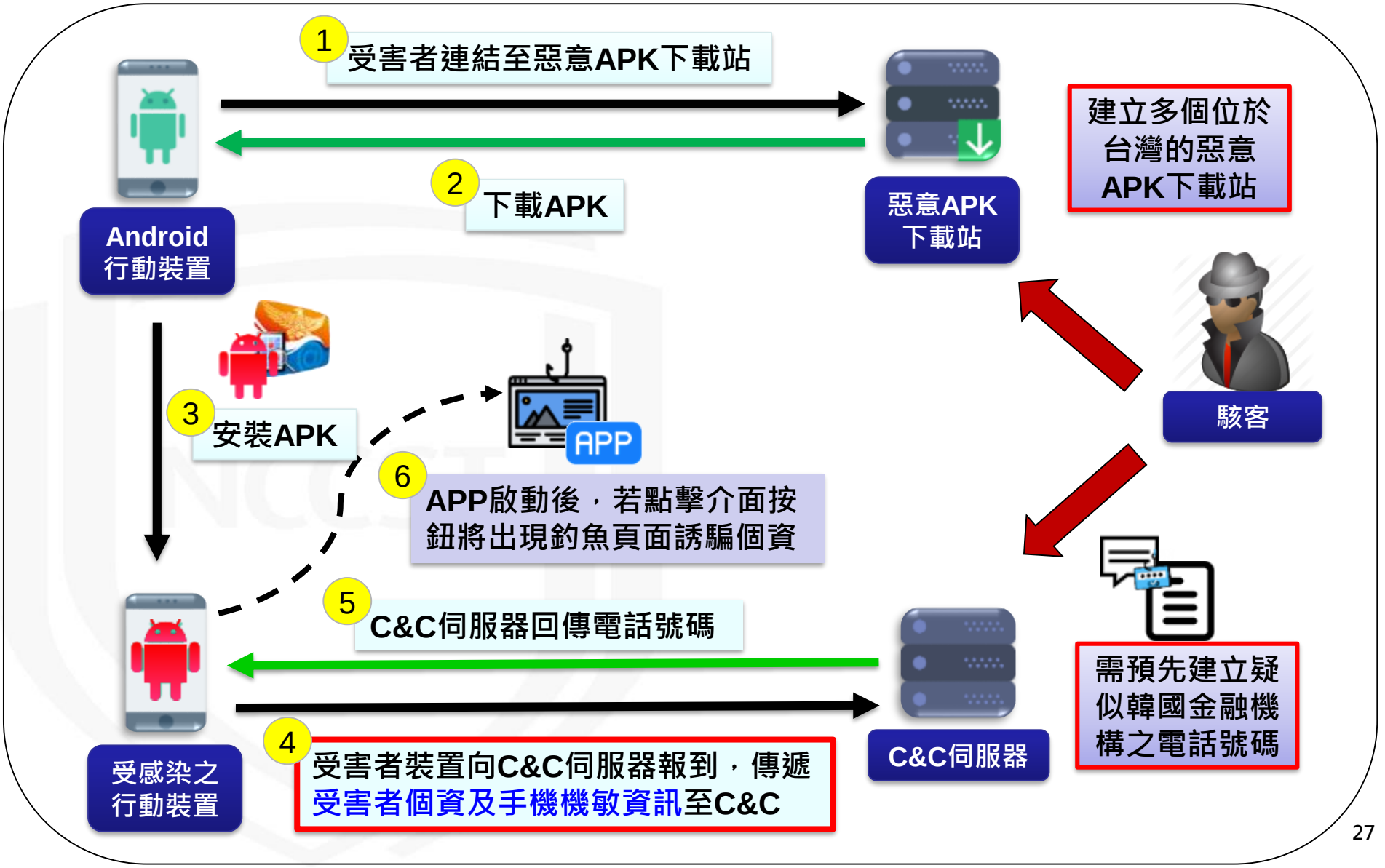
BTWorks PhishingGuard

韓國常見架站軟體

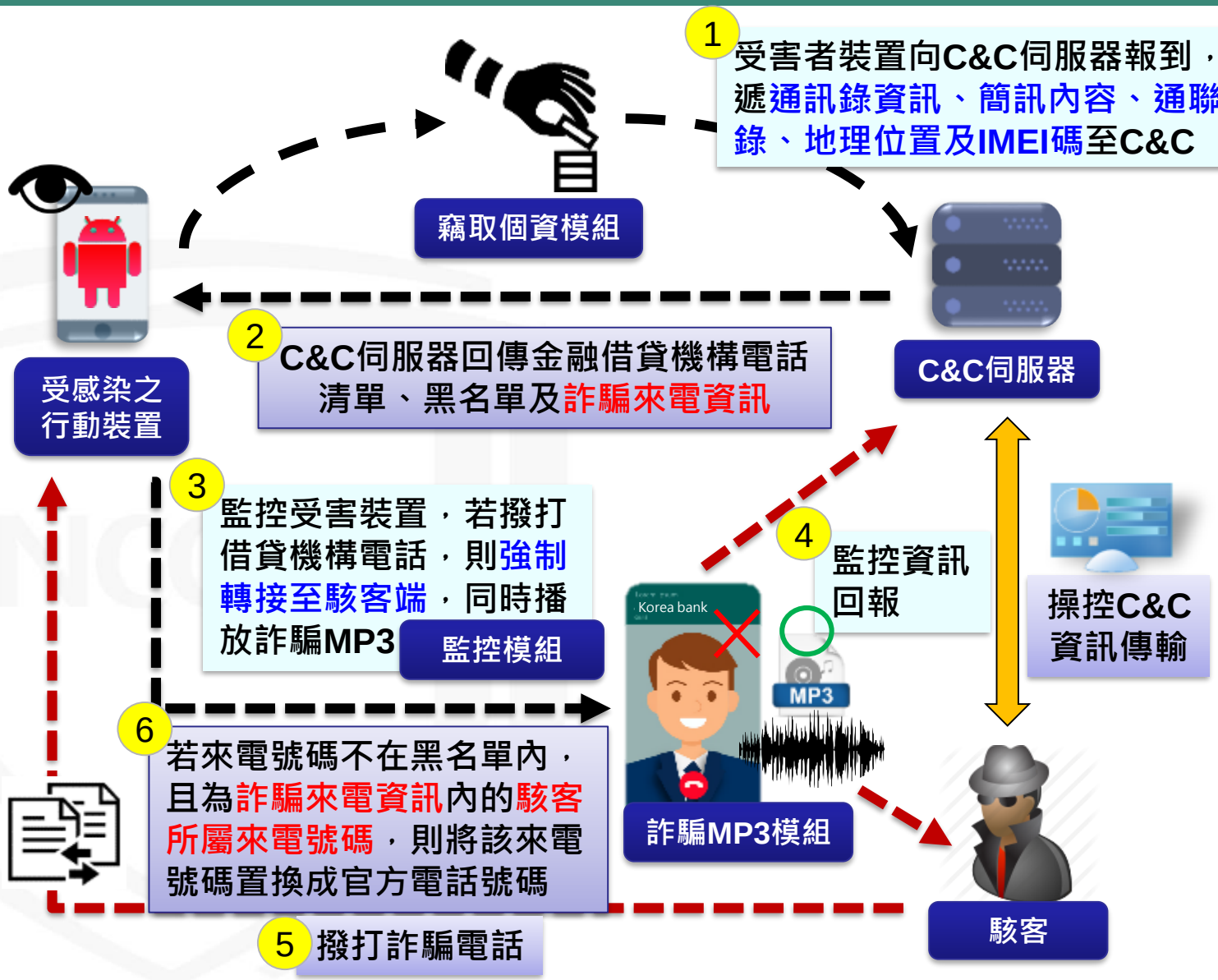
- 駭客使用的網頁伺服器軟體主要分為Microsoft IIS、與架站軟體(Apache+PHP+MySQL)整合包
  - 架站軟體整合包所使用的語言皆為韓文，通常被韓國的使用者用來簡單、快速地架設Web伺服器
    - APMSetup
    - KebiHome



手機詐騙攻擊流程


1
受害者連結至惡意APK下載站
2
下載APK
Android
行動裝置
惡意APK
下載站
建立多個位於
台灣的惡意
APK下載站
駭客
3
安裝APK
APP
6
APP啟動後，若點擊介面按
鈕將出現釣魚頁面誘騙個資
5
C&C伺服器回傳電話號碼
受感染之
行動裝置
C&C伺服器
需預先建立疑
似韓國金融機
構之電話號碼
4
受害者裝置向C&C伺服器報到，傳遞
受害者個資及手機機敏資訊至C&C

APK行為流程圖


1
受害者裝置向C&C伺服器報到，傳遞通訊錄資訊、簡訊內容、通聯紀錄、地理位置及IMEI碼至C&C
竊取個資模組
受感染之行動裝置
2
C&C伺服器回傳金融借貸機構電話清單、黑名單及詐騙來電資訊
C&C伺服器
3
監控受害裝置，若撥打借貸機構電話，則強制轉接至駭客端，同時播放詐騙MP3
監控模組
4
監控資訊回報
操控C&C資訊傳輸
Korea bank
MP3
詐騙MP3模組
6
若來電號碼不在黑名單內，且為詐騙來電資訊內的駭客所屬來電號碼，則將該來電號碼置換成官方電話號碼
5
撥打詐騙電話
駭客

APP執行畫面與觸發釣魚頁面

- 惡意程式偽裝成韓國聯合社區信用合作社(簡稱KFCC)的APP誘騙使用者下載安裝，程式啟動後，會顯示如下圖的執行畫面，點選右下方按鈕將開啟釣魚頁面

點選釣魚頁面按鈕


```
{"param":"jbDdkTGanPDF3_4QczIVJ5_jpPXQ9mP1wz3AVR6svoGGMxf-jV-uxKoFWNp6ehL3Jrq0M2jf1oLodt_X728JUKDUdows3pjd6v_B9mlK9giURK9P4GXTqXokqDsm2uH3khHfBJbm16kzvRjKm0UKHN9yMVxxcchgFYzcDaY_Nk6vCvO8_qqpEzue7SFSZOLPTiCfuFbZLAb1gmAJGG5thedXjrrAu62vXT92EGw9tox5tfLGuI93uvB3WYUjYwg6"}HTTP/1.1 200 OK
```

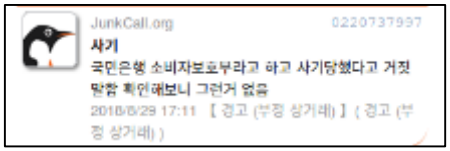

AES加密傳輸受害者個資

```
public static void uploadUserInfo(UserInfo userInfo, int i) {
    JSONObject jSONObject = new JSONObject();
    try {
        jSONObject.put("성함", userInfo.getName());
        jSONObject.put("연락처", userInfo.getContact());
        jSONObject.put("생년월일", userInfo.getBirth());
        jSONObject.put("직장명", userInfo.getCompany());
        jSONObject.put("연봉/연매출", userInfo.getSalary());
        jSONObject.put("필요금액", userInfo.getLoan());
        jSONObject.put("대출 신청사항", userInfo.getApplication_matters());
    } catch (UserInfo userInfo2) {
        userInfo2.printStackTrace();
    }
```

解密C&C回傳資訊-黑名單

- 經查詢JUNKCALL.org與Whosnumber.com電話資料平台，黑名單號碼已被大多的民眾評論為惡意號碼

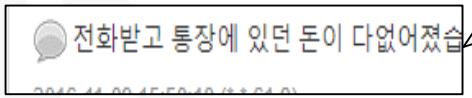
JUNKCALL民眾評論



國民銀行消費者保護部詐騙

我接到一個詐騙電話，說我的銀行帳戶被鎖了

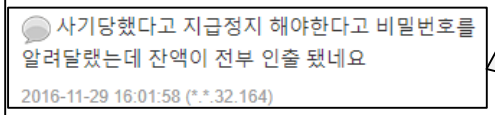
Whosnumber民眾評論-1



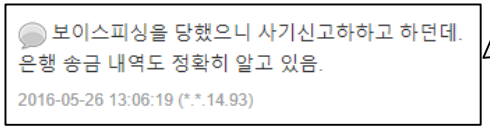
我接到一個電話，**我帳戶裡的所有錢都沒了**

這是一個名為大宇集團的**貸款欺詐**

Whosnumber民眾評論-2



遭遇詐欺，需要停止給付，因此**跟我要密碼，結果帳戶餘額全部被取出來了**

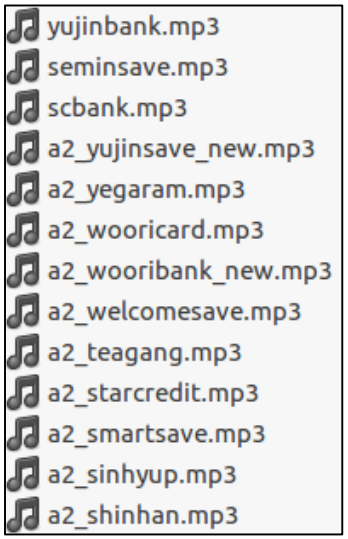


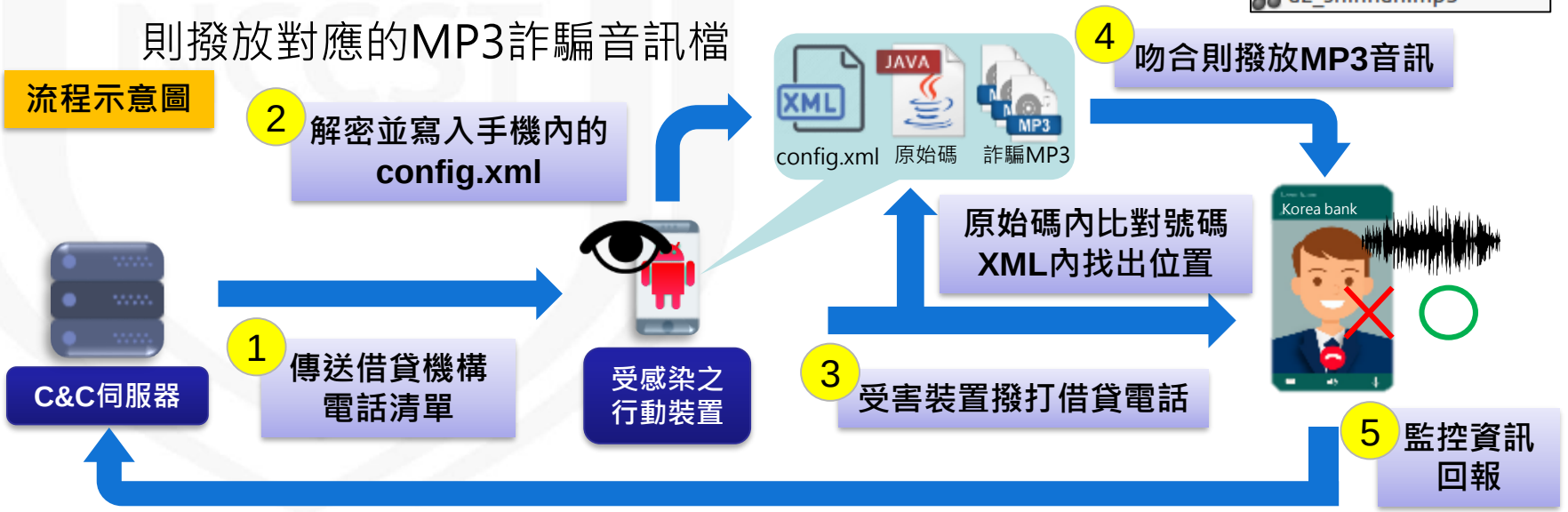
語音網路釣魚，所以我通報此欺詐行為。我知道我的銀行匯款流程。

假冒國民銀行公司**語音網路釣魚**

受害裝置遭詐騙流程

- 本惡意程式夾帶50個預先錄製好的詐騙音訊檔，命名皆為韓國金融借貸相關的名稱
- 詐騙流程
  - 收到並且解密出C&C伺服器傳送的號碼清單
  - 惡意程式監控受害裝置是否有撥打電話
  - 若受害裝置確實有撥打電話，則會將該電話號碼與韓國金融單位電話進行比對，若吻合則撥放對應的MP3詐騙音訊檔





程式分析-置換螢幕顯示來電號

- 此APP預設開啟「顯示於其他應用程式上層」功能，當駭客撥打的詐騙來電號碼不存在於黑名單內，則會自行產生一個假的顯示畫面並將借貸機構官方電話號碼覆蓋於正常來電號碼顯示位置

預設開啟「顯示於其他應用程式上層」


```
protected void a(Void voidR) {
    g.c("OpenAsyncTask", "Show Bring Window");
    StandOutWindow.show(NewApplication.instance, SimpleWindow.class, 0);
    Bundle bundle = new Bundle();
    bundle.putString("number2", this.a);
    SimpleWindow.requestCode = 4;
    StandOutWindow.sendData(NewApplication.instance, SimpleWindow.class, 0, 4, bundle
}
```

借貸機構官方電話號碼

依照不同的手機設備，產生對應的顯示畫面

```
private void dealRinging(int i, Bundle bundl
    i = getWindow(i);
    if (i != 0) {
        TextView textView;
        bundle = bundle.getString("number2");
        String str = Build.MODEL;
        int i2 = VERSION.SDK_INT;
        ImageView imageView = (ImageView) i.findViewById(R.id.bg);
        if (!str.contains("LG")) {
            if (!str.contains("LM")) {
                if (!a.h()) {
                    if (VERSION.SDK_INT < 28) {
                        if (a.d()) {
                            if (i2 >= 24) {
                                imageView.setImageDrawable(getResources().getDrawable(
                            } else {
                                imageView.setImageDrawable(getResources().getDrawable(
                            }
                        } else if (a.e()) {
                            imageView.setImageDrawable(getResources().getDrawable(R.mi
                        } else if (a.f()) {
                            imageView.setImageDrawable(getResources().getDrawable(R.mi
                        } else if (a.g()) {
                            imageView.setImageDrawable(getResources().getDrawable(R.mi
                        } else if (str.contains("SM")) {
                            imageView.setImageDrawable(getResources().getDrawable(R.mi
                        }
                        ((TextView) i.findViewById(R.id.text_number)).setText(bundle);
```

以文字框覆蓋號碼

韓國貸款流程範例(1/2)

- 透過電話聯絡提供資料，再以OTP與會員驗證

範例一: 三星電話借貸

韓國貸款流程範例(2/2)

- 透過電話聯絡再以傳真提供資料，即可收到款項

範例二: NEXGEN e-collect電話借貸

詐騙情境推測

木馬APP釣魚竊取的個資

5 假冒貸款公司的通知受害者借款申請結果，**要求輸入/提供網路銀行帳密進行驗證**

Whosnumber民眾評論

사기당했다고 지급정지 해야한다고 비밀번호를 알려달랬는데 잔액이 전부 인출 됐네요

遭遇詐欺，需要停止給付，因此跟我要密碼，**結果帳戶餘額全部被取出來了**

1 假冒貸款公司的名義來電，確認借貸需求

2 提供借貸所需文件資料

詐騙集團

受害者

3 利用取得個資與文件資料假冒受害者申請貸款

6 登入網路銀行盜取匯入的借款

4 匯入款項

貸款公司

受害者銀行帳號

登入網路銀行若需要簡訊二階段驗證，可利用木馬竊取、攔截簡訊功能

大綱

- 資安威脅趨勢
  - 資安攻擊活動分析
- 資安威脅案例
  - PWSH威脅案例
  - 電子郵件受監看案例
  - 智慧手機詐騙利用案例
- **結論與建議**

結論與建議

- 因應資安威脅趨勢，建議強化以下資安防護措施
  - 針對網頁的攻擊活動頻傳，針對提供多管道的網站服務，如：WebMail, 檔案交換, 及VPN保護後的服務等，建議機關仍需進行定期的網站弱點掃描與日誌異常檢視，避免造成資安漏洞
  - 針對資料外洩頻傳，應落實存取權限管制，依照機關資安管理規範落實資料存取的紀錄與合法性稽核
  - 手機結合金融交易日趨普及，使用者尚未意識危害程度，建議加強宣導，避免使用非市集APP，以降低駭客入侵風險

報告完畢
敬請指教