果核數位
Digicentre

appGuard

2018 Online Shopping Security
Gamania - Digicentre

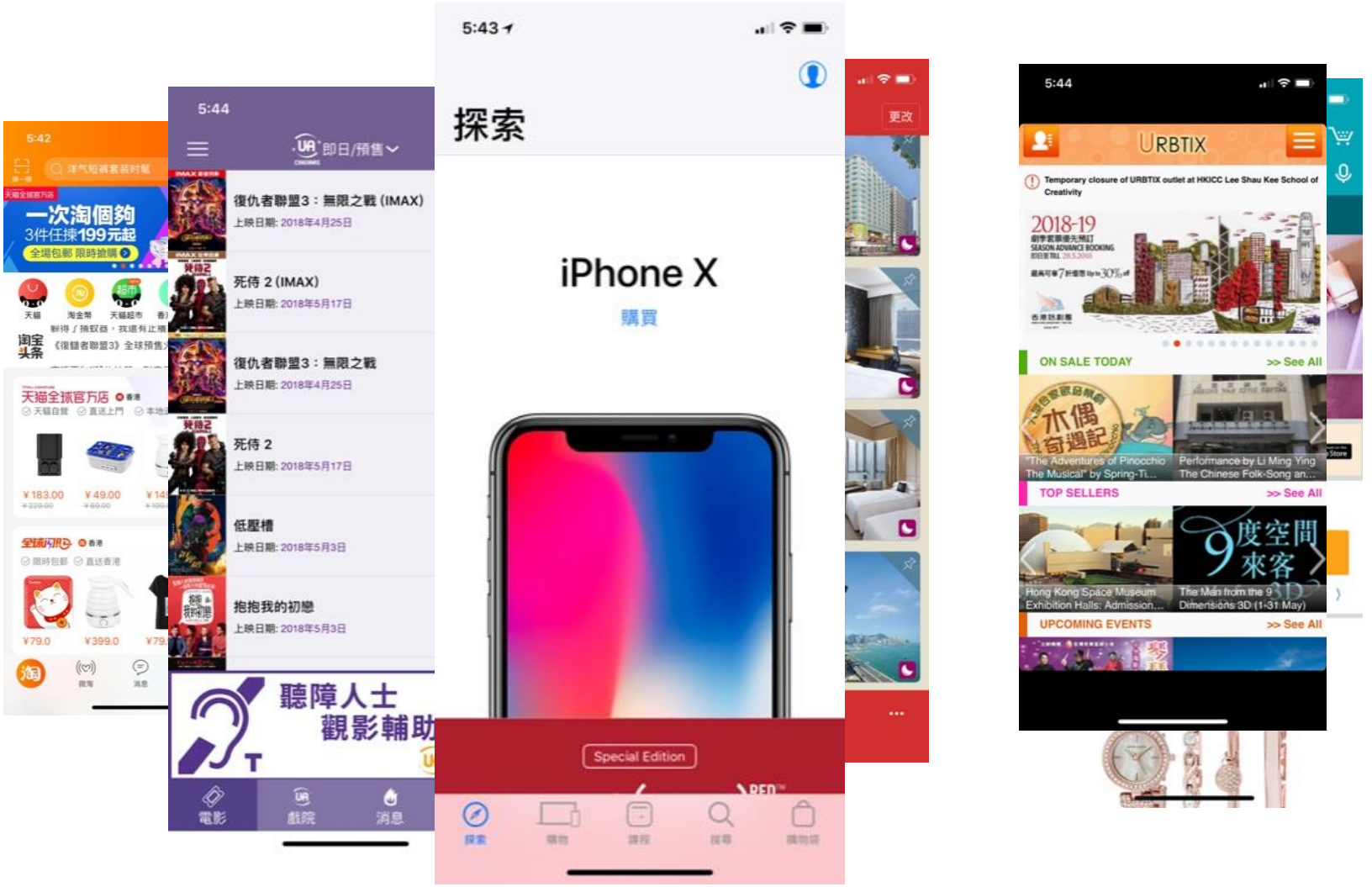
Agenda

- Web Online Shopping & Threat
- Mobile Online Shopping & Threat
- Mobile app Case
- How to prevent

01

Online Shopping

Online Shopping



02

Web Online Shopping & Threat

案例分享

要聞港聞 2018年01月04日 黑客入侵大航假期網盜資料勒索

黑客入侵大航假期網盜資料勒索

11,085

讚 75

AA

【本報訊】再有本港旅行社電腦疑遭黑客入侵，專營內地短線團的大航假期昨晚在網站發通告，指前晚深夜接獲疑似黑客勒索，聲稱已入侵其客戶數據庫套取部份客戶身份證號碼及電話等個人資料，並勒索款項。大航事後報警，但無交代事涉多少客戶，這是繼去年11月黑客入侵縱橫遊的客戶資料庫導致20萬客戶資料外洩後第二宗同類事件。

旅遊業議會總幹事陳張樂怡稱昨接獲大航假期報告事件，對方稱有客戶資料外洩，但初步不涉信用卡資料，大航亦無透露是否有旅行團受影響不能出發。私隱專員公署關注事件，稱收到大航假期資料外洩通報，指遭未經授權人士入侵會員數據庫，包括姓名、身份證及回鄉證資料、電話號碼等個人資料外洩。警方網絡安全調查科正跟進調查。

客戶身份證及電話外洩

大航假期昨晚在網站發出「懷疑黑客非法入侵伺服器盜取會員資料」通告，指本月2日晚上11時許，收到疑似黑客勒索信息，指已入侵其客戶數據庫，導致客戶身份證，回鄉證號碼及電話等資料外洩，並遭對方勒索，即時報警及向個人資料私隱專員公署報告。大航稱重視事件，對受影響客戶深感抱歉，在收到勒索後即時評估並採取應對措施，現正加強網絡保安，並根據私隱專員公署指引

即時新聞 | 報價 | 報章 | 周刊 | 電子報 | 投資 | 中國 | 名家專欄 | TOPick

首頁 | 即時財經 | 即時推介 | 板塊攻略 | 大市 | 名家 | 財金教室 | 行情

【黑客入侵】38萬客戶資料或被盜 香港寬頻：遭超前技術

列印

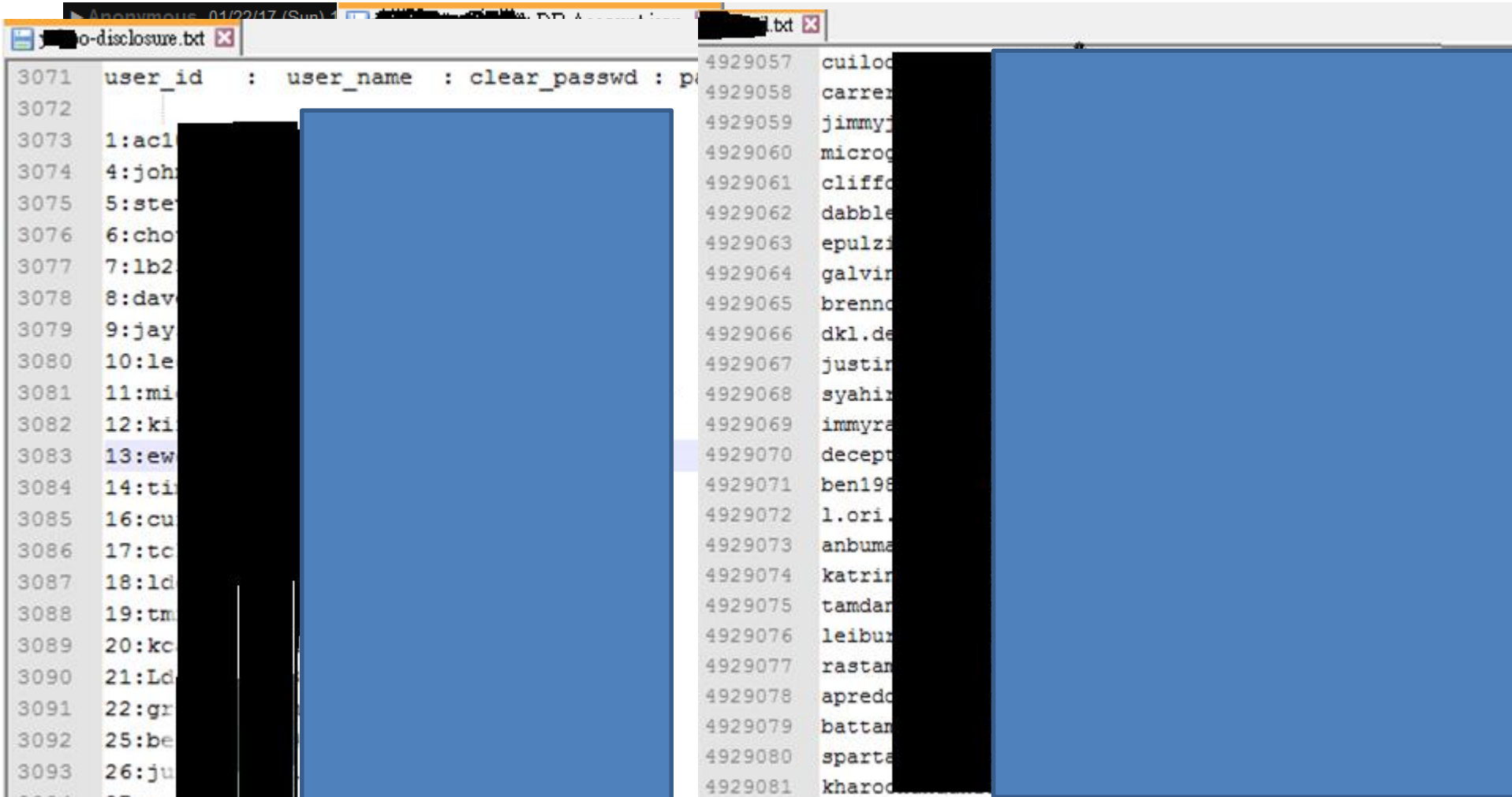
2018年4月18日 18:43 星期三

38萬客戶資料或被盜 香港寬頻：遭超前技術入侵

讚好 0 分享

案例分享-駭客想要什麼

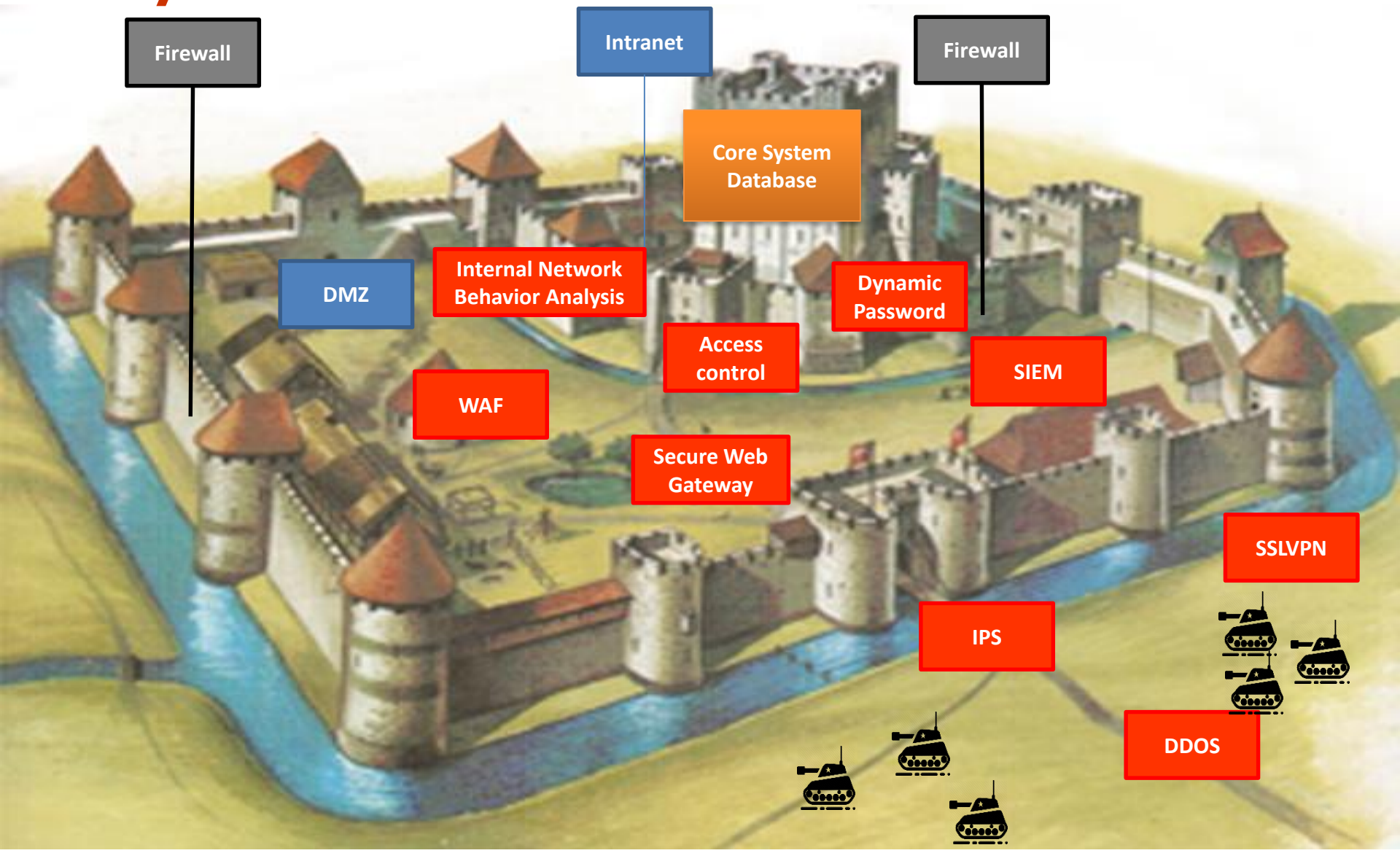
Deep Net



案例分享-駭客攻擊Web application

圖片來源: hp.com

硬體/網路層面強化保安


Firewall
Intranet
Firewall
Core System Database
DMZ
Internal Network Behavior Analysis
Dynamic Password
Access control
SIEM
WAF
Secure Web Gateway
SSLVPN
IPS
DDOS

application 層面強化保安

傳輸安全

APP傳輸需要加密。
透過加密傳輸
降低被中間人攻擊
(HTTPS)

Source code

需針對Source code 做Code Reivew。
透過工具審查，可降低開發時造成的開發錯誤。
(Fortify, Collaborator, GitLab)

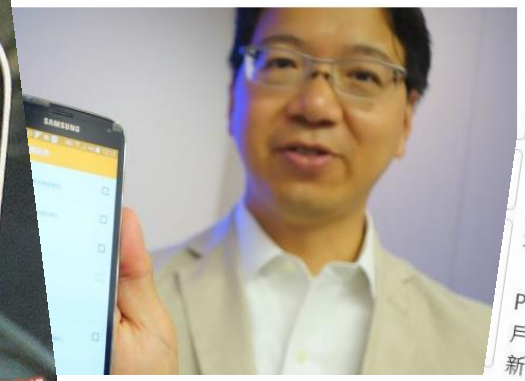
Server side

伺服器端需做VA、PT
透過VA、PT了解伺服器端的問題，降低伺服器端被攻擊風險
(VA、PT)

03

Mobile Online Shopping & Threat

案例分享-手機感染途徑



新型手機銀行木馬程式，殺入香港！銀行木馬程式過往甚少針對某些地區，但專門為香港「度身訂造」的變種木馬程式，例如「Acecard」，近月殺入香港，多人中招。它可偽裝成Google Play、WhatsApp或Line，甚至銀行程式，以認證為藉口，誘騙用戶自拍身份證明文件，還指明要提交香港身份證資料，也有新變種以新加坡為目標。香港金管局證實接獲有銀行報告有關未經授權的網上股票交易，不排除部分是不法之徒，透過流動裝置上的惡意程式竊取進行交易。警方提醒市民，不要下載來源或性質可疑的程式。

案例分享-application感染途徑

案例分享-駭客攻擊途徑

大量發佈
釣魚簡訊

手機被Root
載入病毒

針對特定APP
注入攻擊

丟出假的
APP

丟到非正式
渠道

無法判別是否
正版的user
下載使用

App – 駭客破解流程

是否可以反編譯

否

是否可以監測記憶體

否

放棄 Or 找其他

是

是

看到原始碼

竊取重要資料

動態監測

攻擊成功透過SMS感染

是

是否可以注入

否

放棄 Or 找其他

修改成功丟出修改包欺騙使用者造成傷害

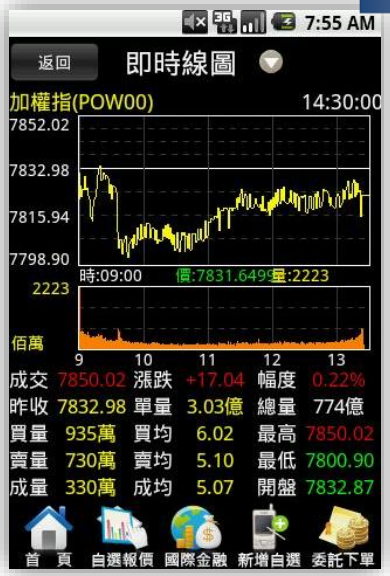
是

是否可以修改

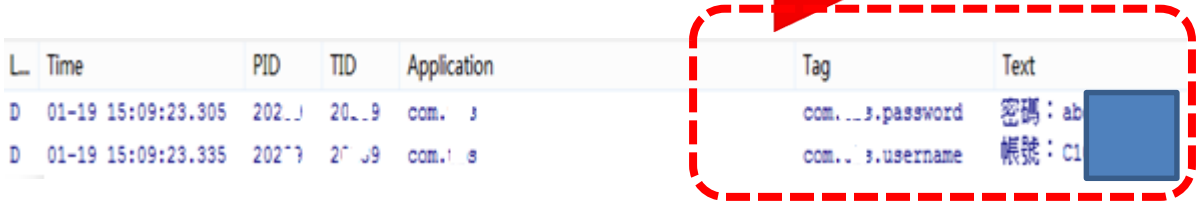
否

放棄 Or 找其他

案例分享-竊取資料(沒有阻擋逆向工程及程式偵錯)



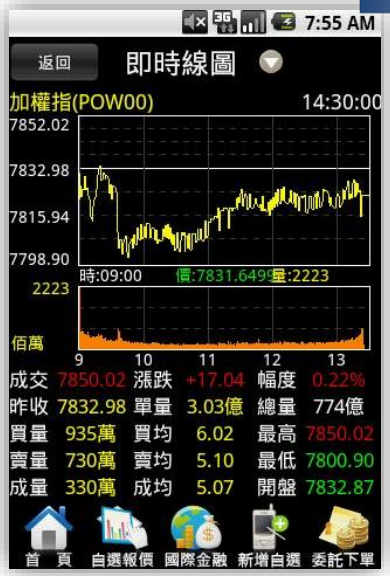
券商下單APP
明碼狀況下 ，了解涵數就可竊取帳號密碼



案例分享-竊取資料(沒有阻檔程式偵錯)

動態植入惡意程式，開始竊取行動

```
root@m0chn:/data/local/tmp # ps | /data/data/tools/busybox grep com.
ps | /data/data/tools/busybox grep com.tbs
u0_a112   10714 17498 [redacted] 401ba664 S com[redacted]
root@m0chn:/data/local/tmp # ./hijack -d -p 10714 -l /data/local/tmp/l[redacted]rmon.s
o
data/local/tmp/l[redacted]rmon.so
mprotect: 0x401b9454
dlopen: 0x400abef9
pc=401ba664 lr=400d23f5 sp=bef95110 fp=bef952a4
r0=ffffffc r1=bef95130
r2=10 r3=1db
stack: 0xbef75000-0xbef96000 leng = 135168
executing injection code at 0xbef950c0
calling mprotect
library injection completed!
```



取得帳號密碼

案例分享-修改APK(沒有防二次打包)

```
text:73605298                   sub_73605298
text:73605298 FC 30                             ADDS    R0, #0xFC
text:7360529A 41 63                             STR     R1, [R0,#0x34]
text:7360529C 70 47                             BX      LR


73605298                sub_73605298
73605298 FC 30                          ADDS    R0, #0xFC
7360529A 40 63                          STR     R0, [R0,#0x34]
7360529C 70 47                          BX      LR
7360529C                ; End of Function sub 73605298
```

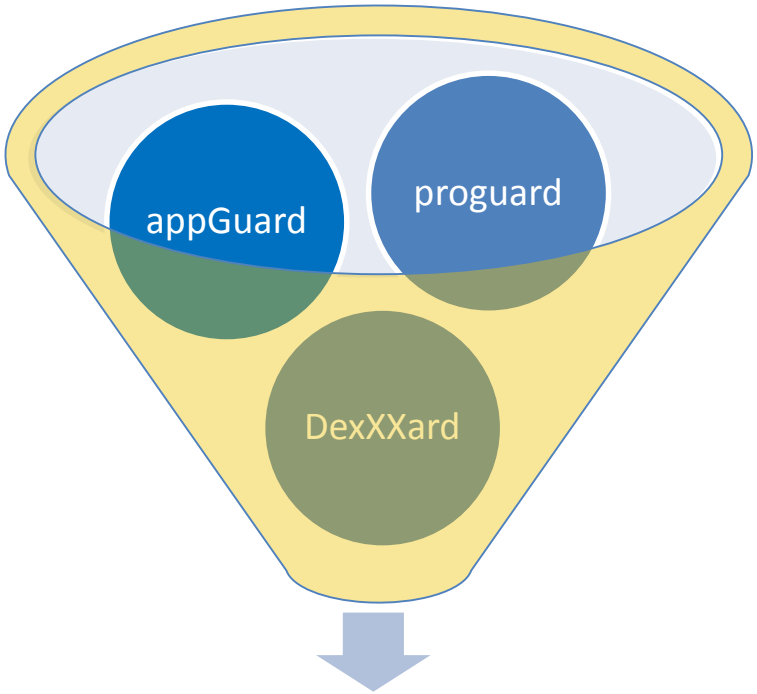
調整修改

04

How to prevent – mobile app

How to prevent – mobile app保護

第三方保護方案



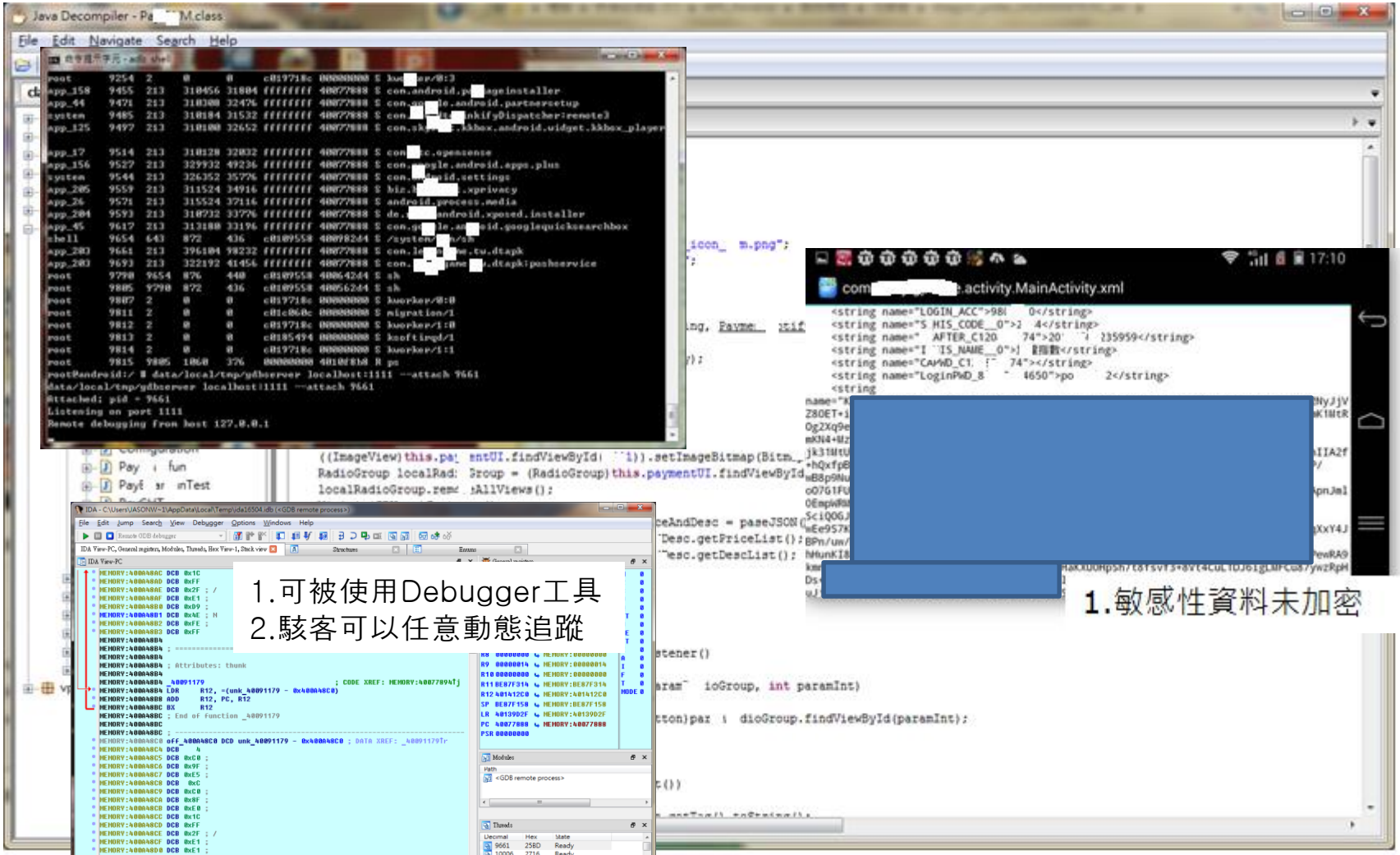
Encryption / Obfuscation

加密保護/混淆保護

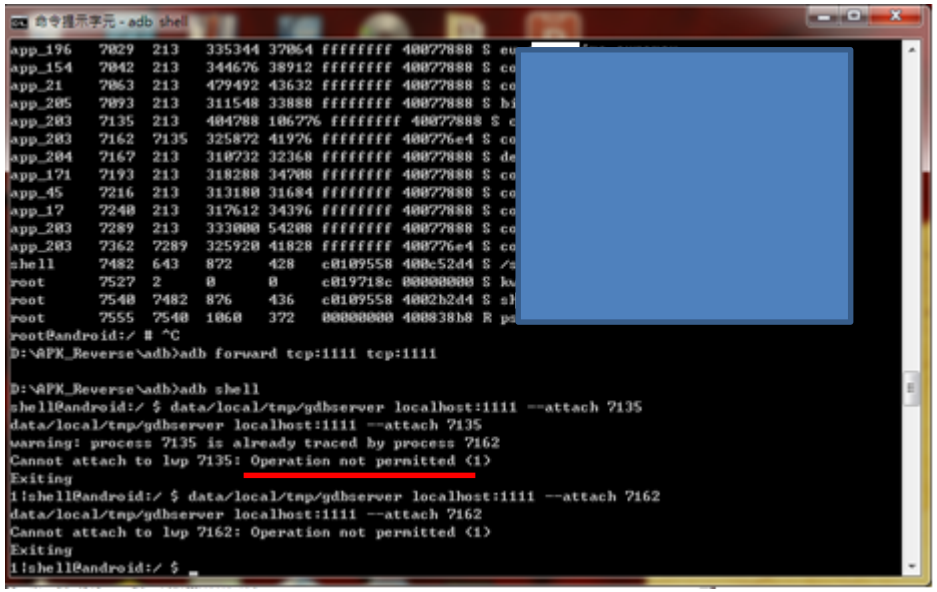
05

保護後的效果

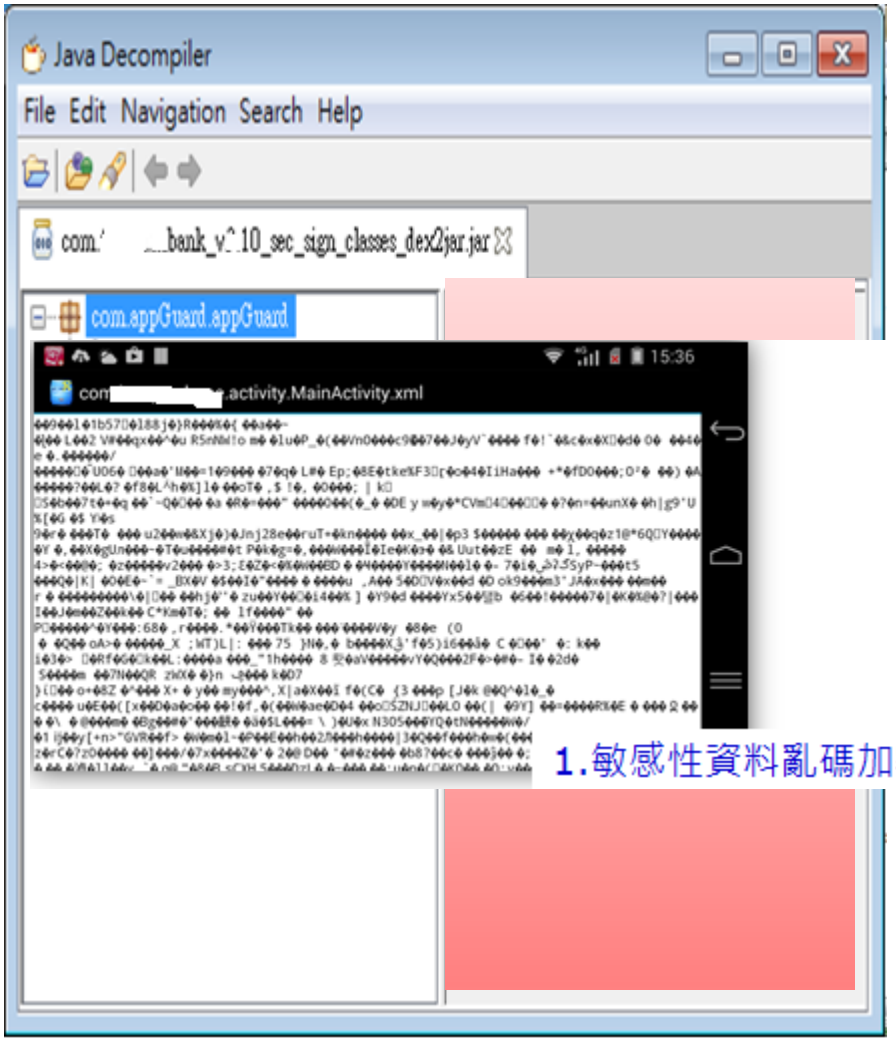
● 沒有保護的狀況



動態追踪及debugger 都不能使用



加密效果



06

Q&A