



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



apple daily.com.hk

AA

f t

【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奪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 北

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：遭超前技術入侵



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

黑客入侵範圍

涉及客戶：**38萬**(固網及IDD服務)

涉及資料：

- 地址
- 電話號碼
- 身份證號碼
- 4.3萬條信用卡資料

香港寬頻
HONG KONG BROADBAND NETWORK

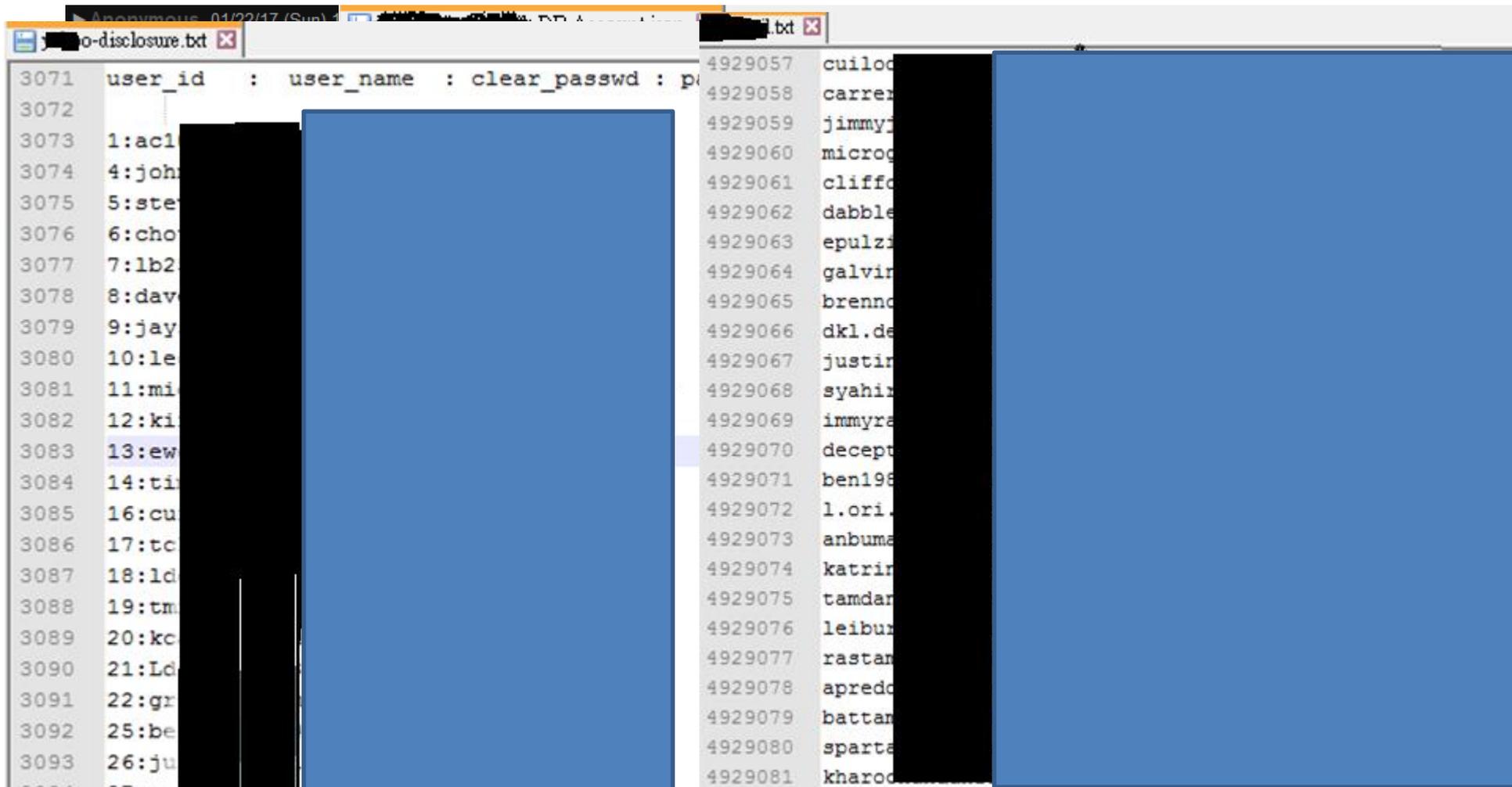
香港寬頻38萬客戶資料被盜

f hket.com

hket

案例分享-駭客想要什麼

Deep Net



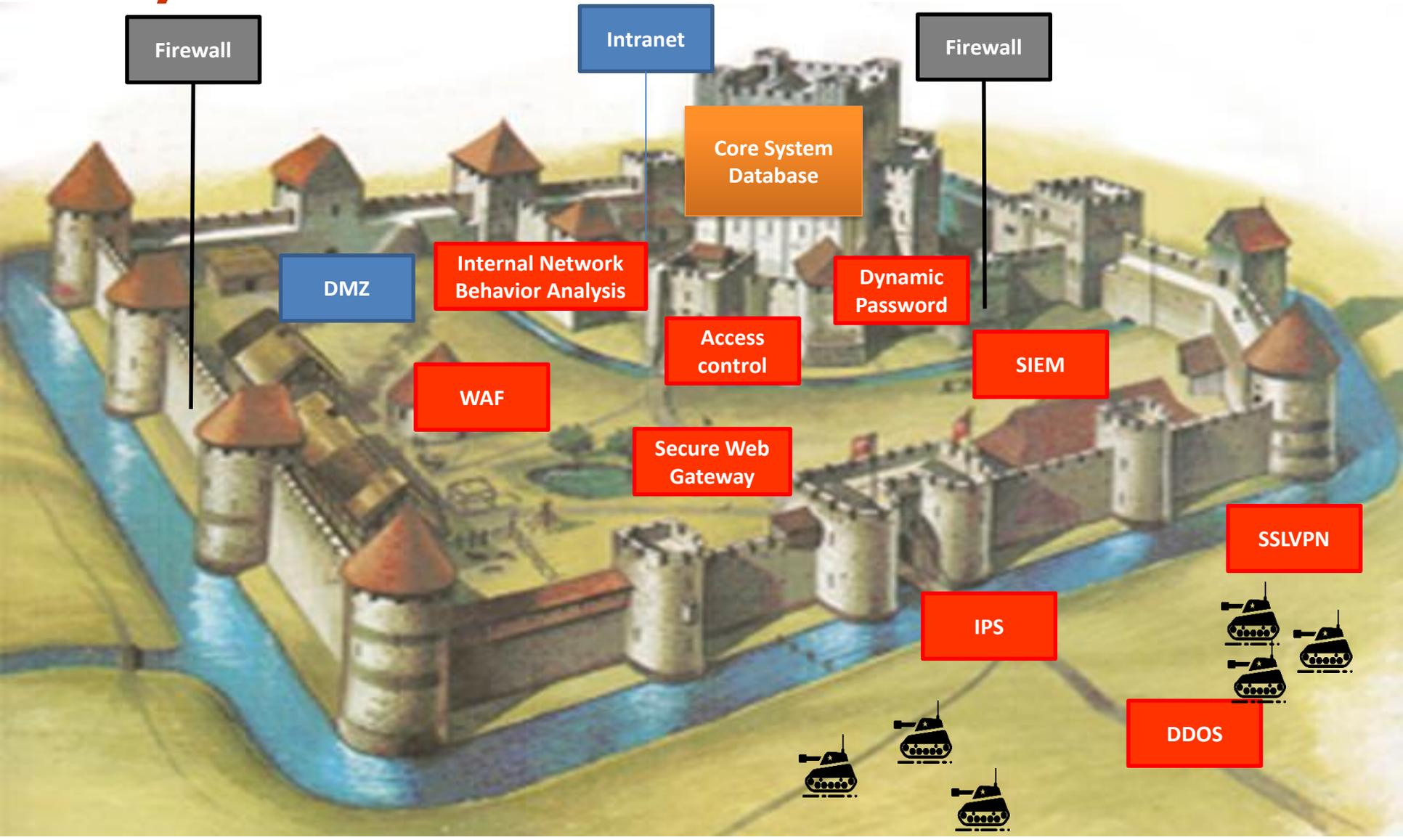
The image shows a terminal window displaying a list of user accounts. The columns are labeled 'user_id', 'user_name', 'clear_passwd', and 'p'. The data is partially redacted with black boxes. The visible user names include: cuilod, carren, jimmyj, microg, cliffc, dabble, epulzi, galvir, brenno, dkl.de, justin, syahin, immyra, decept, ben198, l.ori, anbuma, katrin, tamdar, leibur, rastan, aprede, battan, sparta, and kharod.

user_id	user_name	clear_passwd	p
4929057	cuilod		
4929058	carren		
4929059	jimmyj		
4929060	microg		
4929061	cliffc		
4929062	dabble		
4929063	epulzi		
4929064	galvir		
4929065	brenno		
4929066	dkl.de		
4929067	justin		
4929068	syahin		
4929069	immyra		
4929070	decept		
4929071	ben198		
4929072	l.ori		
4929073	anbuma		
4929074	katrin		
4929075	tamdar		
4929076	leibur		
4929077	rastan		
4929078	aprede		
4929079	battan		
4929080	sparta		
4929081	kharod		

案例分享-駭客攻擊Web application



硬體 / 網路層面強化保安



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



資訊保安

保安專家示範木馬入侵盜取資料 莫乃光呼籲市民提防黑客短訊

資訊保安 by Boris Lee on 八月 14, 2015 · add comment

FACEBOOK TWITTER GOOGLE+ LINKEDIN



有朋友對哪些內容讚好，
聞，除了來自電話外，最近亦流傳在 WhatsApp 和 SMS 短訊出現駭客惡意
司資訊保安專家呼籲市民，提防不明來歷的短訊，以免被木馬程式套取手
即場展示了黑客入侵的示範。



專門為香港「度身訂造」的變種木馬程式，近月殺入香港，多人中招。

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

首頁 話題 精明消費 健康 親子 休閒 職場 新聞 商業解碼

YAHOO! 新聞
雅虎香港

搜尋

搜尋新聞

搜尋網頁

首頁 視像 港聞 兩岸國際 財經 娛樂 體育 天氣 健康 親子 副刊 專欄 熱門搜尋 新聞app

易被黑客盜私隱 近半Android買股App存漏洞

晴報 晴報
2017年8月4日 8:50

7 則留言



港研會來港多市民

【晴報專訊】近3月前的18個月，股票交易應用程式香港無線科技商會當期聯交所列表所，輕易複製加密鑰匙。

- 黑客攻陷證券行App 挪900萬炒高仙股
 - http://hk.on.cc/hk/bkn/cnt/news/20160917/bkn-20160917033054001-0917_00822_001.html
- Hackers targeted stock trade mobile app (STMA), hacked user account and made 9M unauthorized transactions, pushed penny stocks. User lost 2M dollars.

Google Play Store出現假WhatsApp 全球逾100萬人

11/06 讚好 1,044



Google Play Store出現假WhatsApp 全球逾100萬人中招

早前全球斷網後，近日又有假WhatsApp出現在Google Play Store，全球逾100萬人中招。有網民發現打開「假WhatsApp」後，發現它不斷出現廣告，建議用戶

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

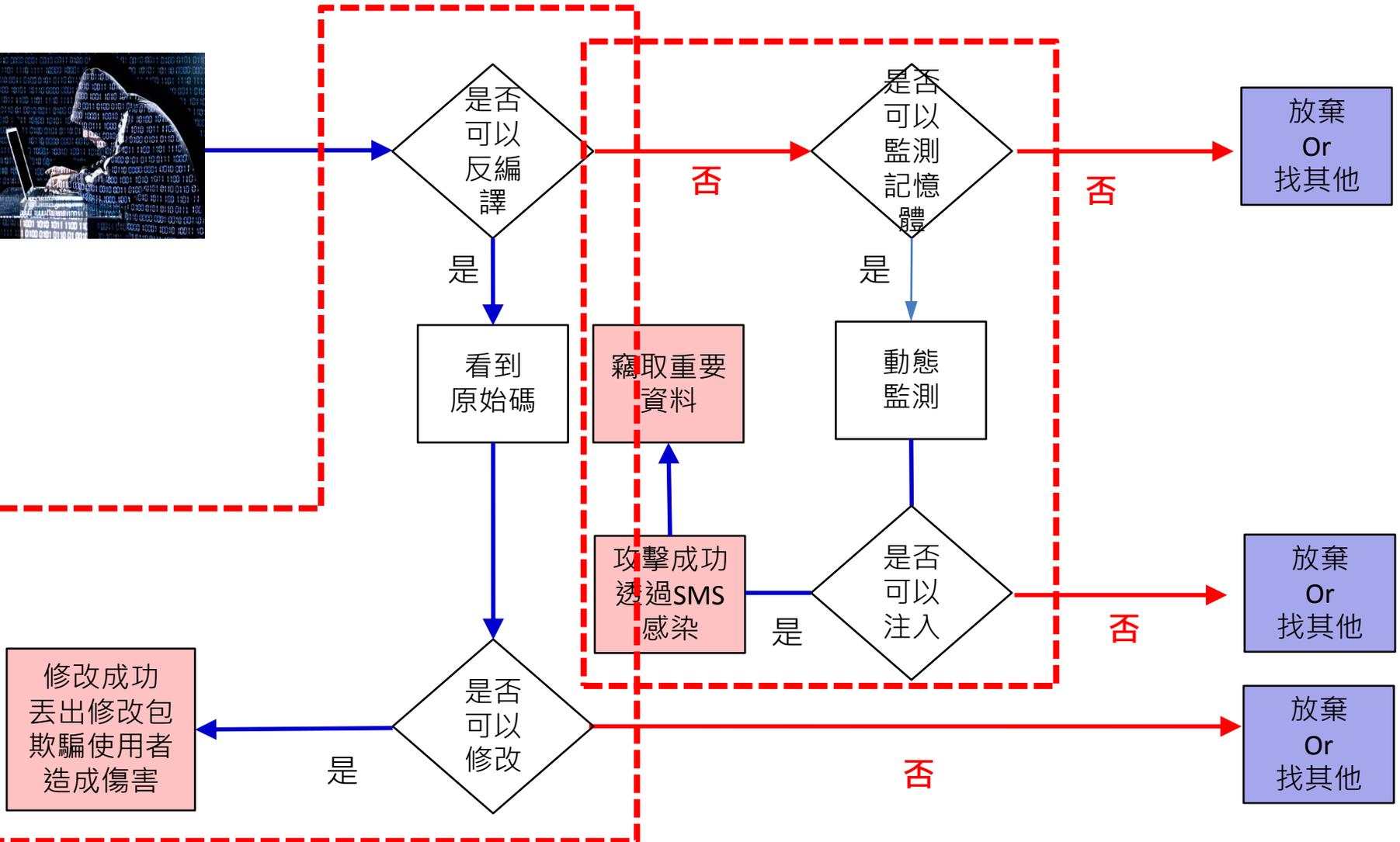


丟到非正式
渠道



無法判別是否
正版的user
下載使用

App - 駭客破解流程



案例分享-竊取資料(沒有阻擋逆向工程及程式偵錯)



```

public static String login(String paramString1, String paramString2, String paramString3, String paramString4, String paramString5, String paramString6)
{
    StringBuffer localStringBuffer = new StringBuffer();
    localStringBuffer.append("FORM=");
    localStringBuffer.append("VER=");
    localStringBuffer.append("PID=");
    localStringBuffer.append("CODE=");
    localStringBuffer.append("TIME=");
    localStringBuffer.append("ID=");
    localStringBuffer.append("SID=");
    localStringBuffer.append("AC=");
    localStringBuffer.append("FARM=");
    localStringBuffer.append("FCO=");
    localStringBuffer.append("FCO=");
    localStringBuffer.append("PWCTYPE=");
    localStringBuffer.append("CASO=");
    localStringBuffer.append("CACO=");
    localStringBuffer.append("CADATE=");
    localStringBuffer.append("VAR=");
    return localStringBuffer.toString();
}
    
```

券商下單APP
明碼狀況下，了解函數就可竊取帳號密碼

L	Time	PID	TID	Application
D	01-19 15:09:23.305	202...	20...9	com...
D	01-19 15:09:23.335	202...	2...9	com...e

Tag	Text
com...password	密碼: ab
com...username	帳號: C1

案例分享-竊取資料(沒有阻檔程式偵錯)

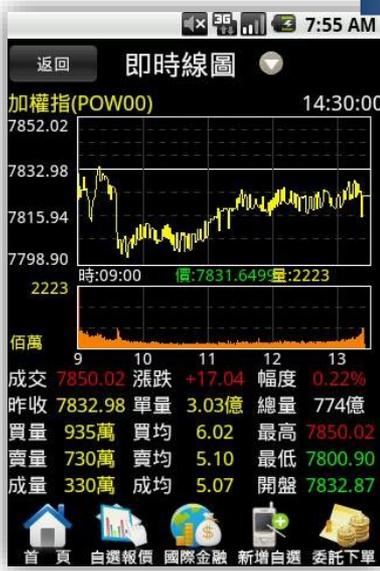


動態植入惡意程式，開始竊取行動



```

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



```

sb20.toString() = com.[REDACTED]account.TP [REDACTED] D [REDACTED]
sb20.toString() = 密碼:abr [REDACTED]
sb20.toString() = /data/data/com.[REDACTED]/databases/
mitake.sqlite
sb13 = /data/data/com.[REDACTED]/databases/[REDACTED].sqlite
sb13.equalsIgnoreCase() = 0 :memory:
sb13 = /data/data/com.[REDACTED]/databases/[REDACTED].sqlite
sb13.equalsIgnoreCase() = 0 :memory:
sb13 = /data/data/com.[REDACTED]/databases/[REDACTED].sqlite
sb13.equalsIgnoreCase() = 0 :memory:
sl
sl
sb9 = /data/data/com.[REDACTED]/databases/mitake.sqlite
sb9.endsWith() = 0 webViewCache.db
sb9 = /data/data/com.[REDACTED]/databases/[REDACTED].sqlite
sb9.endsWith() = 0 internal.db
sb9 = /data/data/com.[REDACTED]/databases/[REDACTED].sqlite
    
```

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
text:7360529A 41 63
text:7360529C 70 47

73605298          sub_73605298
73605298 FC 30
7360529A 40 63
7360529C 70 47
7360529C          ; End of Function sub_73605298
    
```

ADDS R0, #0xFC
STR R1, [R0,#0x34]
 BX LR

ADDS R0, #0xFC
STR R0, [R0,#0x34]
 BX LR

調整修改



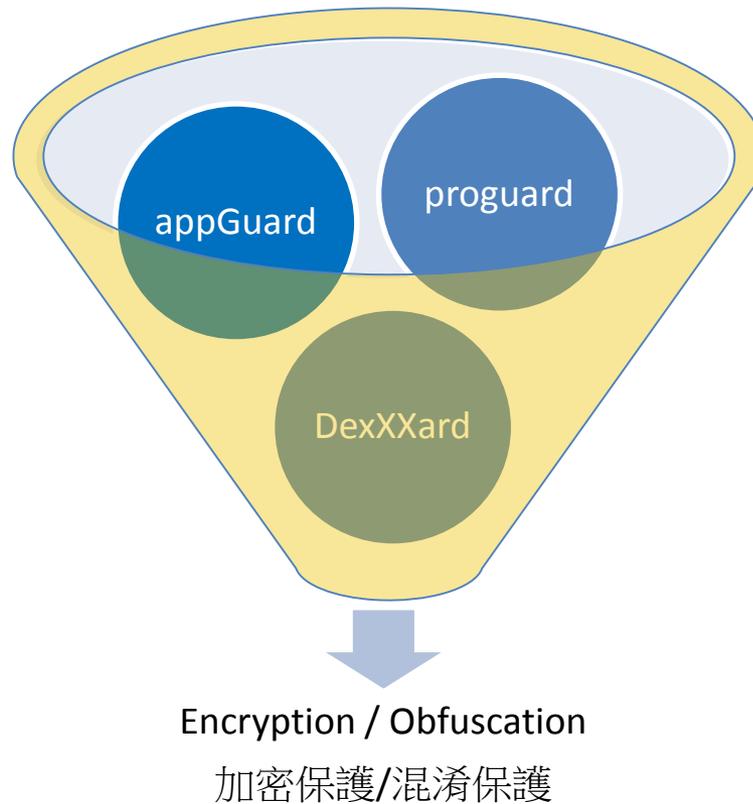
04

How to prevent – mobile app



How to prevent – mobile app保護

第三方保護方案

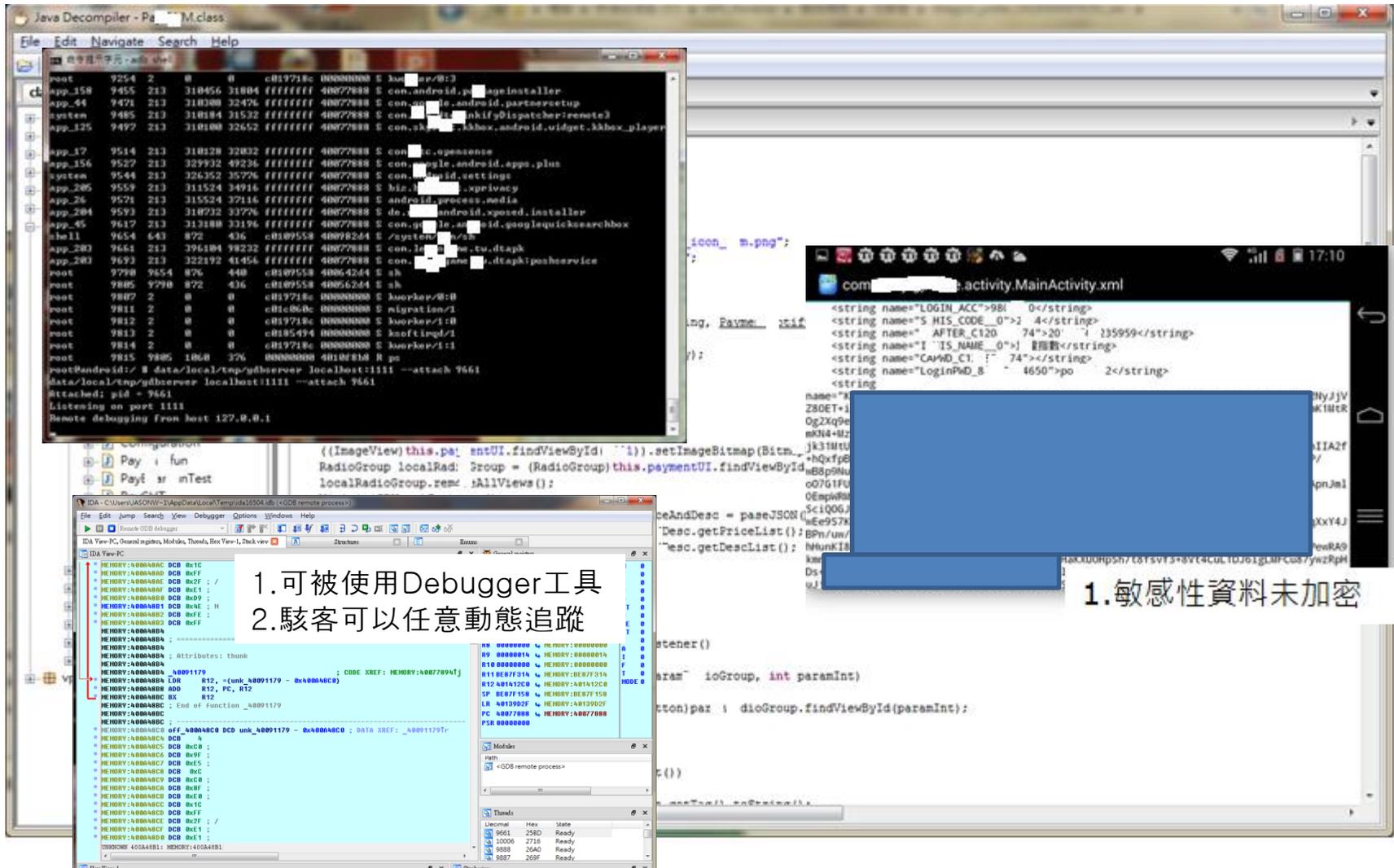


05

保護後的效果



沒有保護的狀況



The collage illustrates the lack of protection in an Android application. It shows how sensitive information, such as a PIN and password, is stored in plain text within the application's resources (XML files). Additionally, it demonstrates how a debugger can be used to dynamically track and intercept data during runtime.

1. 可被使用Debugger工具
2. 駭客可以任意動態追蹤

1. 敏感性資料未加密

06

Q&A



