

# 資訊通犯罪概況與未來挑戰



USERNAME:

Administrator

PASSWORD:

LOGIN

警政署刑事警察局  
電偵大隊 隊長莊明雄  
2020.11

# 講師介紹

• 姓名：**莊明雄 (RICHARD) SB**

• 現職 (Present Position)：

**刑事警察局電信偵查大隊 隊長**

• 學歷 (Education)：

警察大學刑事所碩士、臺灣科技大學資管博士候選人

• 經歷 (Experience)：

1. 刑事局**偵九隊**(全國最早成立網路偵查隊)偵查員、偵查正

2. 刑事局**科技犯罪防制中心研發科**(中央級網路策略單位)警務正、組(股)長

3. 警政署**165反騙專線**(全國反詐騙專責)股長兼主管

• 著作：網站入侵現場鑑證實錄 (基峰出版社)

• 專業 (Specialty)

國安會、法務部、司法官學院、法官學院、憲兵學校、移民署、海巡署、警大、警專、資策會等單位講師、行政院防治網路詐騙專案小組成員，並取得NSPA、CEH、CHFI等資安證照，曾受派前往美國、德國、葡萄牙、韓國、越南、印尼、菲律賓、中國大陸等國與當地警方交流~



# Out Line

- 👤 資安問題非一日形成
- 👤 打擊犯罪需要新方法
- 👤 巧婦難為無米炊的困境
- 👤 資安的等於國安的期望



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



# 虛擬VS現實

黑客攻擊

電影的情節是否會發生??

電力、水力、核能  
電視台、電信業者  
網路犯罪問題僅止於  
電腦?





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境

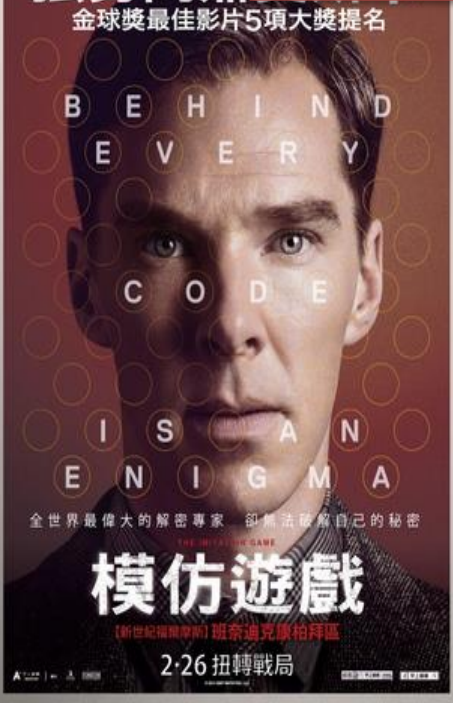


資安的等於國安的期望

強勢問鼎

金球獎最佳影片5項大獎提名

小小的數讀(Sudoku)測驗也能破解德軍密碼!



HISTORY HOLLYWOOD.COM - THE IMITATION GAME





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

高中畢業

警專

警察大學

基層拔擢

積分

考試

外部晉用

特考(二、三、四)

警大(二技、研究所)

國內警察來源很多元





資安問題非一日形成



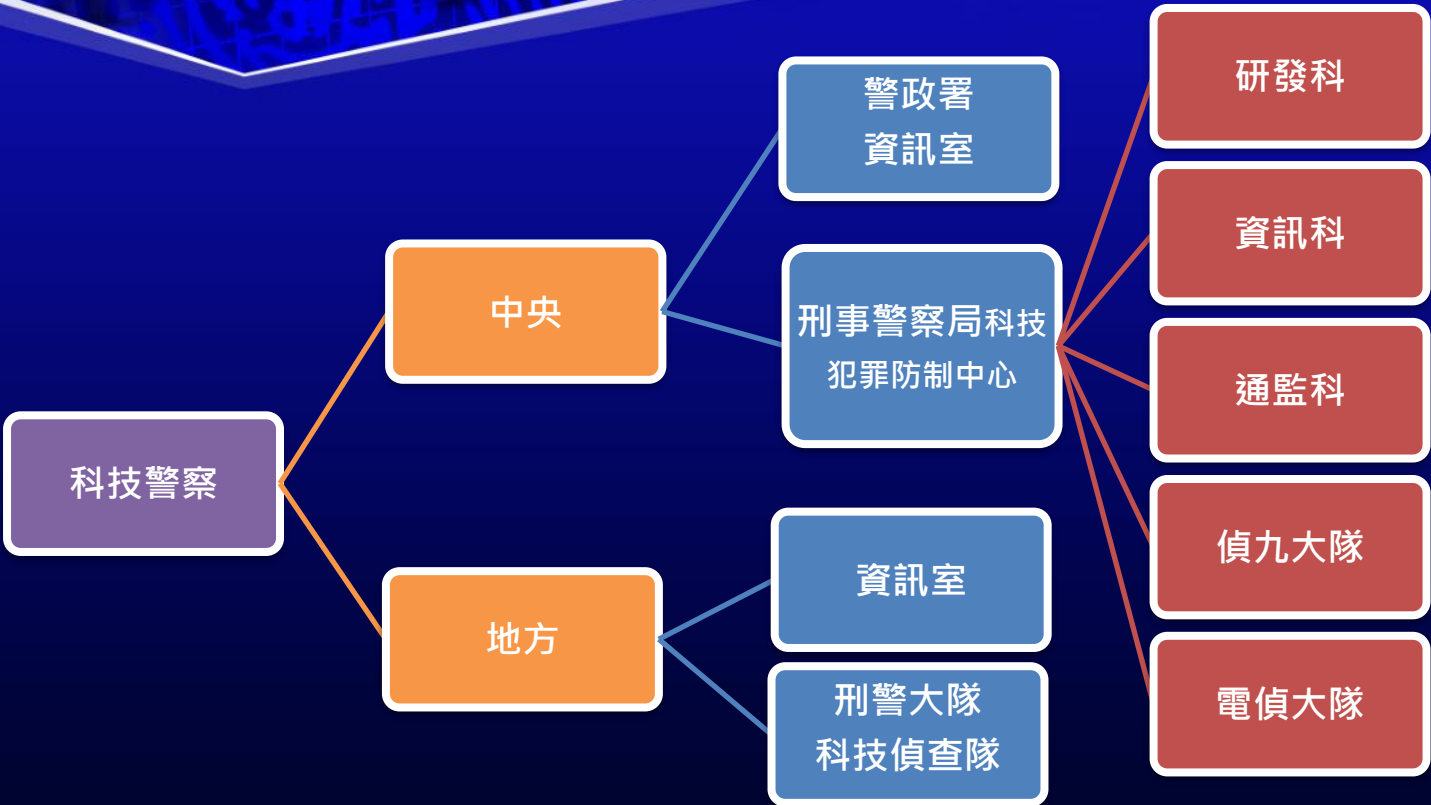
打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望





資安問題非一日形成



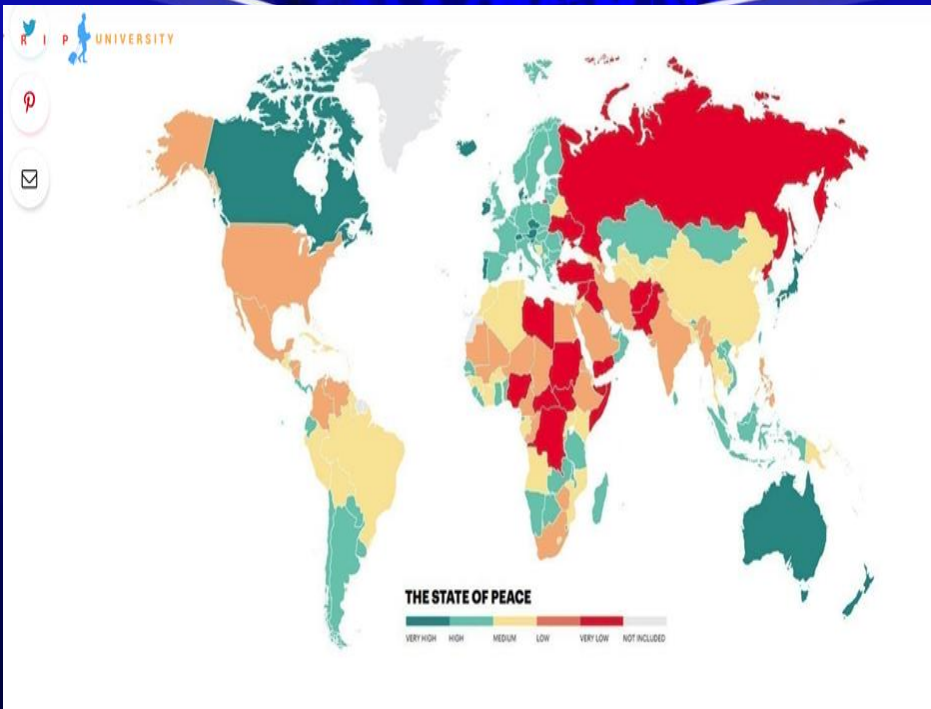
打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



全球最大數據庫「Numbeo」13日公布最新全球治安排名，**臺灣為全球第2安全、犯罪率倒數第2低的國家**，僅次於中東國家卡達，同時也打敗日本、新加坡、北歐各國等以治安良好著稱的國家。

全球治安最差、犯罪指數最高的國家前10名，依序則為**委內瑞拉**、巴布亞紐幾內亞、南非、阿富汗、宏都拉斯、千里達及托巴哥、巴西、圭亞那、薩爾瓦多及敘利亞。

<https://www.chinatimes.com/newspapers/20200714000424-260106?chdtv>





## 資安問題非一日形成



## 打擊犯罪需要新方法



## 巧婦難為無米炊的困境



## 資安的等於國安的期望

### Fortinet 發布全球威脅型態報告，揭台灣病毒威脅比全球更嚴重

作者 Nana Ho | 發布日期 2020 年 08 月 27 日 22:54 | 分類 網路, 資訊安全

讚 322 分享



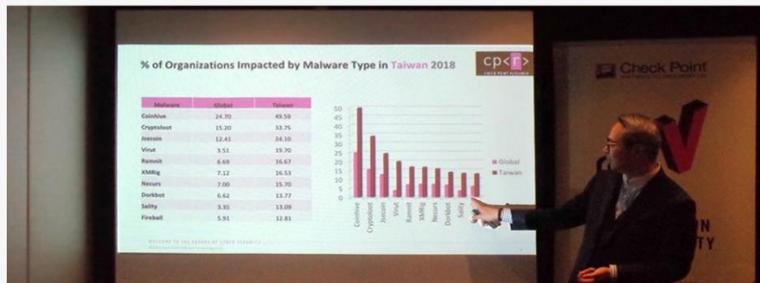
iThome 新聞 產品&技術 專題 AI 區塊鏈 Cloud DevOps GDPR 資安 研討會 社群 商用電腦

### 臺灣遭受惡意程式攻擊現況揭露，竟是Botnet攻擊最多國家

最新惡意程式攻擊趨勢出爐，2019年初臺灣遭受Lokibot與Virut的攻擊次數是全球的6倍，Check Point並指出，即便是2018全年臺灣最常見的十大惡意程式，其攻擊次數與比例也都是全球的两倍。

文/ 羅正漢 | 2019-03-07 發表

讚 438 分享



遠傳助企 提升市場

我有

iThome S

你和其他 37 位朋友都

iThome Sec

### 傳 Garmin 伺服器遭到惡意攻擊，台灣產線與美日韓多項服務暫停

作者 陳冠英 | 發布日期 2020 年 07 月 24 日 12:40 | 分類 穿戴式裝置, 資訊安全, 軟體, 系統

讚 766 分享



### 中油遭受勒索軟體攻擊，部分付款方式暫停使用

加油站遭到顧客鎖定並發動攻擊，現在正在臺灣真實上演。許多臺灣中油加油站於中午出現異常，該公司也隨後發出新聞稿，證實他們被勒索軟體攻擊，導致消費者僅能使用現金或信用卡付款

文/ 馬峻佑 | 2020-05-04 發表

讚 加入 iThome 粉絲團

新聞

2020-05-04 15:01 台灣中油公司

台灣中油加油站因遭受惡意程式攻擊資訊系統異常 加油站暫時僅使用現金及信用卡交易

點閱數: 686

台灣中油公司因遭受惡意程式攻擊，感染勒索病毒，目前加油站加油部分受影響者為無法使用捷利卡、中油PAY等相關作業，請消費者加油先使用現金及信用卡，其餘生產和供應並未受到影響。

台灣中油指出，資訊系統今天出現操作異常，目前資訊單位已緊急處理中，儘速排除障礙；消費者大部分使用的現金及信用卡交易不受影響，唯牽涉台灣中油內部系統的相關作業如捷利卡、中油PAY等暫停使用，請消費者改用現金或信用卡支付。

圖片來源: 即濟部



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



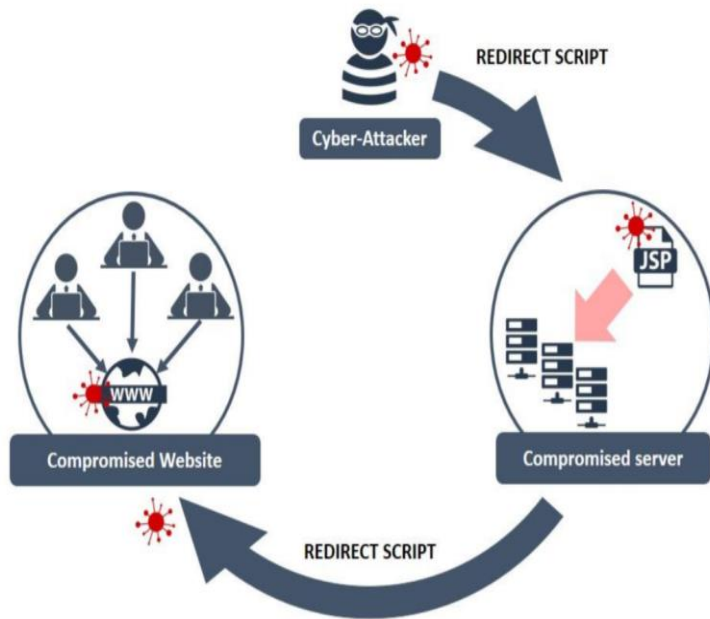
資安的等於國安的期望

# supply-chain attack 供應鏈攻擊

華碩爆資安漏洞！駭客透過系統更新植入後門病毒，百萬台電腦恐受害

2019/03/26

 郭家宏





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 英國航空遭駭案，駭客可能只用22行程式碼就偷走38萬名乘客個資

英國航空被駭一案，研究人員研究其網站，發現Modernizr函式庫被竊改，植入22行惡意程式碼，在使用者於網站上提交付款資訊時，竊取相關資訊及用戶名稱，疑為Magecart駭客集團所為。

文/ 陳曉莉 | 2018-09-12 發表

讚 5.4 萬

按讚加入iThome粉絲團

讚 244

分享

駭客找出 Model 3 安全漏洞！特斯拉：車你直接帶回家吧

2019/03/25

讚 921 分享



電動車綁定「手機」專家破漏洞：APP入侵可操控

2016/07/22 15:24

字級： 字 字





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

### 銓敘部資安重大疏漏 59萬筆文官個資外洩



### Taiwan Ministry of Civil Service 590k leaked

by sonewbye - 06-21-2019, 09:31 AM

Pages (7): 1 2 3 4 5 ... 7 Next >

sonewbye



只賣8歐元

Advanced User

Posts: 40  
Threads: 9  
Joined: Feb 2017  
Reputation: 0  
2 YEARS OF SERVICE

Contents

Toggle

Downloads:

You must register or login to view this content.



資安問題非一日形成



打擊犯罪需要新方法




巧婦難為無米炊的困境



資安的等於國安的期望

About 104



104聲明，35筆資料遭駭皆為2013年舊資料

針對媒體報導，人力銀行個資遭駭一事，104人力銀行初步了解，駭客公開的35筆資料，都是2013年的舊資料。104人力銀行已主動向調查局報案，積極協助調查，並於網站公告相關訊息。

資安是一件永無止盡的防護工程，104人力銀行近年來已於管理面通過 ISO 27001 資訊安全管理與 BS 10012 個人資訊管理制度驗證，並於資安防護技術實踐縱深防禦之佈建，包括：源碼檢測、弱點掃描、滲透測試、資料遺失偵測、端點攻擊防禦、入侵偵測防禦、日誌分析、網路與網站應用程式防火牆等，相關工程並已獲得以下獎項肯定：

- 2018榮獲「資安品質精銳獎」
- 2019榮獲「資安人才培育獎」

104人力銀行將持續強化資安建設，保護使用者個資安全。若求職者仍有疑慮，可諮詢104人力銀行客服人員(02)29126104\*2。

台灣1111人力銀行\*335萬個人詳細信息 (新料) [复制链接]

发表于 2020-10-\*\* | 只看大图 ▶ 楼主

暗网交易论坛  
全球唯一的中文暗网  
担保交易平台，交易无忧！

尚未设置封面图或  
下方查看附件图片  
No-pictures

台湾1111人力銀行\*335萬個人詳細信息 (新料)

售價 1000 美元 市场参考价5000.00

仅剩9件 已售出1件

浏览人气: 1044 次

请确认物品与卖家描述是否一致，卖家如果恶意欺诈，买家可发起投诉或申请退货退款。

立即购买 查看已购物品

购买用户	数量	购买金额	状态	购买时间
oizeaz9	1件	1000美元	购买成功	2020-10-**

之前发布的 [台湾104人力銀行\\*592萬個人詳細信息](#) 防止泛滥，仅余最后一份 \_\_2020.10.05

本次介绍，比104更好的资料，更详细，更新。  
**仅售10份，防止泛滥。**

内容：身份证号、姓名、性别、出生年月、身高、体重、血型、电话、手机、邮箱、住址、毕业院校、专业、个人简历等等。  
非常详细，非常新。  
日期：2019年

数据量：3350000+  
字段名：



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 近期物聯網資安議題層出不窮



白牌 WebCAM 缺乏資安機制遭破解  
個人隱私全都露



陸資企業採用中國製監視器  
引發消費者疑慮



政府採用中國製監視器引發爭議

資料來源  
趨勢科技



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 萬物聯網，處處都存在資安威脅



### 人造衛星

- 2018賽門鐵克揭露Thrip駭客組織使用中國境內的3台電腦，駭入美國與東南亞的衛星通訊業者、電信業與國防承包商。
- 入侵目的主要為攔截通訊，並以匿蹤方式隱藏。



### 飛機

- 2017年美國國土安全全部透露，已於2016年9月成功駭入波音757商用飛機，所使用的方法是利用大多數飛機都會用的無限通訊。
- 2019年初，一位英國資安教授，利用英航客機座位的USB插槽，接上滑鼠讓機上聊天系統當機。



### 汽車

- 2015年，知名資安研究員Charlie Miller示範遠端控制行駛中的吉普車，可控制其音響、雨刷、油門與剎車等。
- 2018年，臺灣資安研究員相繼在臺灣資安大會示範汽車安全研究成果，可控制引擎存取權，於車外強制更新韌體。



### 心律調整器

- 2012年，資安專家Barnaby Jack示範在50呎距離內，駭入心律調節器的無線通訊，製造出830伏特的瞬間電壓。
- 2017年，亞培針對46.5萬臺售出的心律調節器，提供已修補軟體漏洞的新版韌體呼籲用戶連絡醫生以升級軟體。

資料來源  
趨勢科技



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

最新

2019.04.10 19:08

# 瑞典最新調查：台灣受「假新聞攻擊」全球第一

文 | 編務組



全文朗讀

00:00 / 01:06



瑞典V-Dem跨國調查 最新資料  
台灣榮登「外國輸入假資訊」嚴重程度世界第一

TL;DR

Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news

By James Vincent | Apr 17, 2018, 1:14pm EDT

## DeepFace 可能淪為新問題



Source Sequence



Our Reenactment (Full Head)



Averbuch-Elor et al. 2017





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 不能說的秘密?

MSN盜用~~ 全世界第二

臉書盜用~~~全世界第五

LINE盜用~~~全世界第一





資安問題非一日形成



打擊犯罪需要新方法

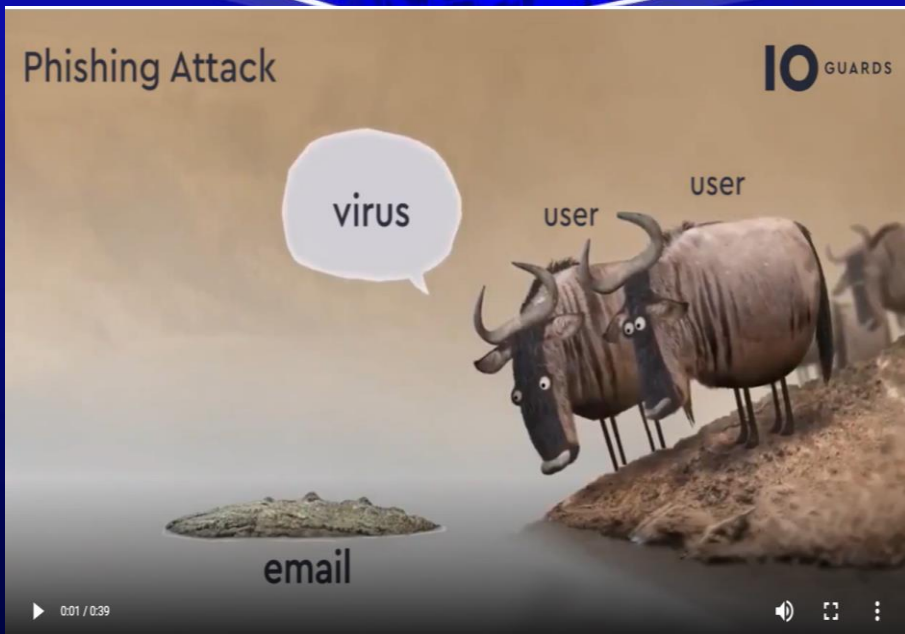


巧婦難為無米炊的困境



資安的等於國安的期望

Administ a





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



1.竊取個資，蒐集資料假冒身分詐騙。



2.繞過身分驗證機制弱的網站，盜(創)用帳號。



3.入侵通訊軟體、電子郵件，假冒身分。



4.攻擊結合惡意程式散布及加密勒索軟體。

進化



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 六顆能量寶石



技術能力

工具運用

知識經驗

勤奮不懈

人緣好

絕佳運氣



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 某旅行社被當跳板?

- 發現從台灣IP
- 網路頻寬很大

某銀行信用卡盜刷

某個公司發送

- 行業相關
- 不排除懷疑

- 被害人
- 涉案人

犯罪懷疑?

## 案例1



Port 9188

116.11.28.XXX(廣西南寧)  
 21.33.70.XXX(四川)  
 71.27.32.XXX(福建)



175.182.XXX.XXX  
 (X旅行社-中華固IP)

Port 9223



112.121.XX.XX  
 112.121.XX.XX



資安問題非一日形成



打擊犯罪需要新方法



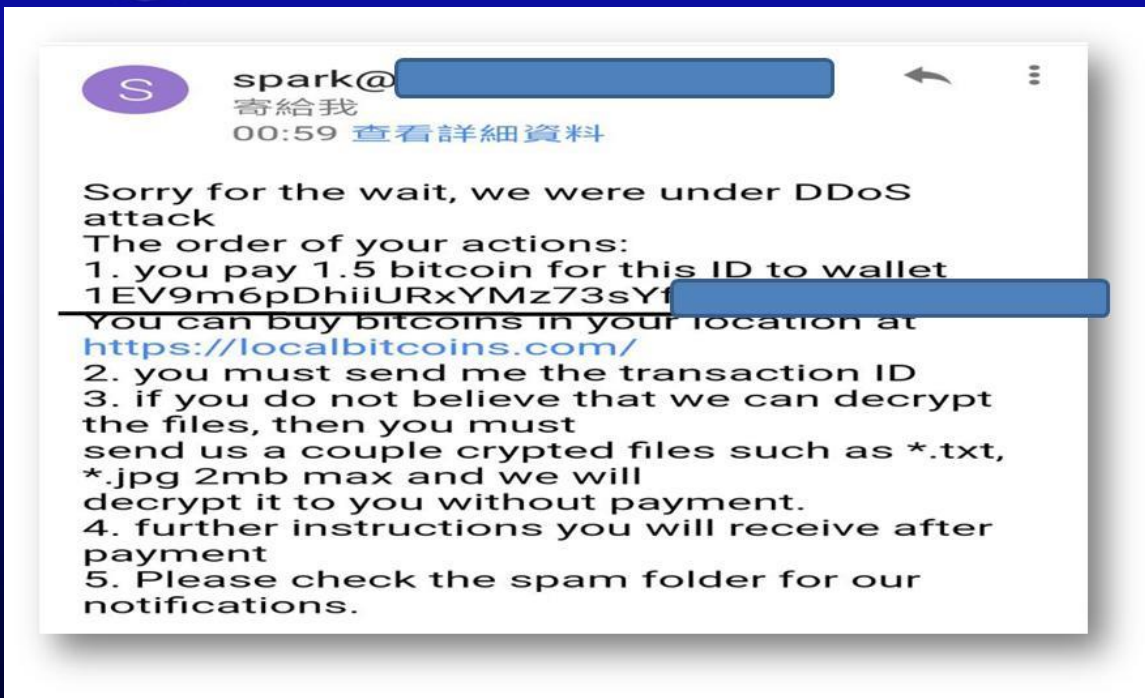
巧婦難為無米炊的困境



資安的等於國安的期望

# 歹徒以比特幣勒索恐嚇信

## 案例2





資安問題非一日形成



打擊犯罪需要新方法



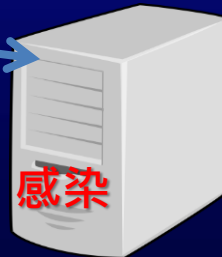
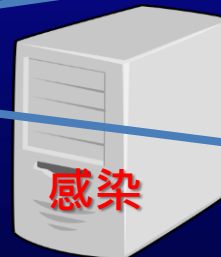
巧婦難為無米炊的困境



資安的等於國安的期望

# 感染途徑

提供遠端登入用電腦遭入侵



當成中繼主機  
2XXX:c048:9f1::c048:9f1  
192.72.9.XXX

電腦  
(員工)

主要勘察電腦





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 壞人會自己加密自己?

名稱	修改日期	類型	大小
AITEMP	2019/1/27 上午 1...	檔案資料夾	
share_mac	2019/1/26 下午 0...	檔案資料夾	
[redacted]	2019/1/26 下午 0...	檔案資料夾	
[redacted].[spark@airmail.cc].btc	2019/1/26 下午 0...	BTC 檔案	643,975 KB
FILES ENCRYPTED.txt	2019/1/29 下午 0...	文字文件	1 KB
Photoshop Temp2156724440	2018/6/14 上午 0...	檔案	0 KB
			0 KB
			141,764 KB
			93 KB





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 比特幣區塊鏈公開查詢機制

**BLOCKCHAIN**    [WALLET](#)    [DATA](#)    [API](#)    [ABOUT](#)        [GET A FREE WALLET](#)

bc9724272eae8ecc9949853d79a83d47722bb5f78617869e55928b5a0789a8	2019-01-29 13:04:18
1EV9m6pDhiiURxYMz73sYfUkBKyeA2SCKK	→ 1HyQdxDJRWeTp2XWaxS9eQ62xAQ2ZFq4Vm 1CZbtCUXhPRXygtTjBvXVqSUoMYaYfnX
	0.35227599 BTC 1.06768772 BTC <b>-1.42 BTC</b>
7267f07045de6ace5ea0fa34264b9caf2f9f319115bdfab1d92d5a20d8c878e5	2019-01-29 02:45:25
371GtsG11UqQKpyYLRUYZKtXMXnZWdFpsA 3HWiqDhFazRdsNeJV47Eq7SuUfuxqcmxR8 38AfCr3dEa9TZzqhm6HtFpKGpoycqGZim9 3Lnr8WNQzsEexfzE9oyFyMfeovVsxDRgD 39ci8dnRJysPuHgeRY83b5vDRJqeksVeud 32NJJDPJnKbCdWmtCxpH8gxiPpQhbNnxa 39aR79VCFaKWUxXCfsssFnoGYcaqsjKvCf 3DwooFN83oPFhvVz2q4EyceGtes4SAnCUz 39d68FBtVQsM4aemrgp2t2r1c84oTYPd	→ 1EV9m6pDhiiURxYMz73sYfUkBKyeA2SCKK
	1.42 BTC



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 假遊戲點數網站樣態



案例3

釣魚網站是竊取的信用卡資料很普遍的犯罪手法，網站製作非常類似真實難辨真假！



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



香港商報

7月28日

## 香港新加坡警察御馬行動

警破跨國「一條龍式釣魚電郵」詐騙集團拘5人

【香港商報訊】記者區天海報道：警方首次搗破跨國「一條龍式釣魚電郵」詐騙集團，本年7月初警方商業罪案調查科、網絡安全及科技罪案調查科連同新加坡警方商業事務局展開代號「御馬」行動，拘捕5名男女。

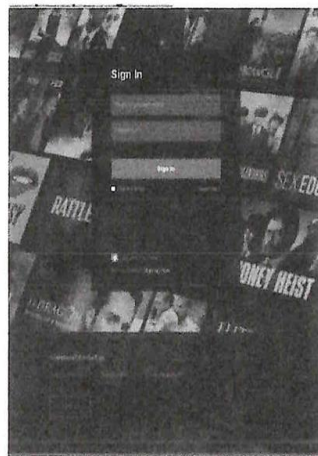
商業罪案調查科署理總警司鄭麗琪表示，在5月收到新加坡警方通知，指有當地市民的信用卡資料被盜用，並在本港的電器連鎖店網購，經深入調查後，鎖定1個以本港為基地的犯罪集團，涉發放大量的釣魚電郵，聲稱網絡電視的使用者需更新資料，當市民進入電郵中的超連結後，被誘使輸入信用卡號碼，騙徒隨即用資料進行網購，買入昂貴的產品，包括電話和電腦等，再轉售圖利。

涉案集團至今已進行150宗交易，涉及款項約130萬港元，被盜取信用卡人士包括美國、法國、新加坡和香港，並已確認21名新加坡市民被盜資料。在本月6日，警方在油麻地、西營盤和屯門拘捕2摩洛哥男子和3名本港女子(26至37歲)，相信是集團骨幹成員，涉嫌「串謀詐騙」，稍後在昨日加控其中1名摩洛哥男子和1名本港女子涉嫌「不誠實取用電腦」，其餘3人已獲准保釋。行動中凍結85萬元資產，相信是部份犯罪得益。警方指在搜查疑犯寓所時，發現電話、電腦和打印機，以及在其中1部電腦中，發現有20億人的個人資料，來自全球40多個國家和地區，當中有電郵地址和證明，部份附有電話號碼和地址等。



寄送假冒Netflix、蘋果、spotify及PayPal的電子郵件，然後利用釣魚詐騙民眾個人資料與信用卡號，透過其他平台購買高金額商品(容易轉賣)

假線上支付網頁





資安問題非一日形成



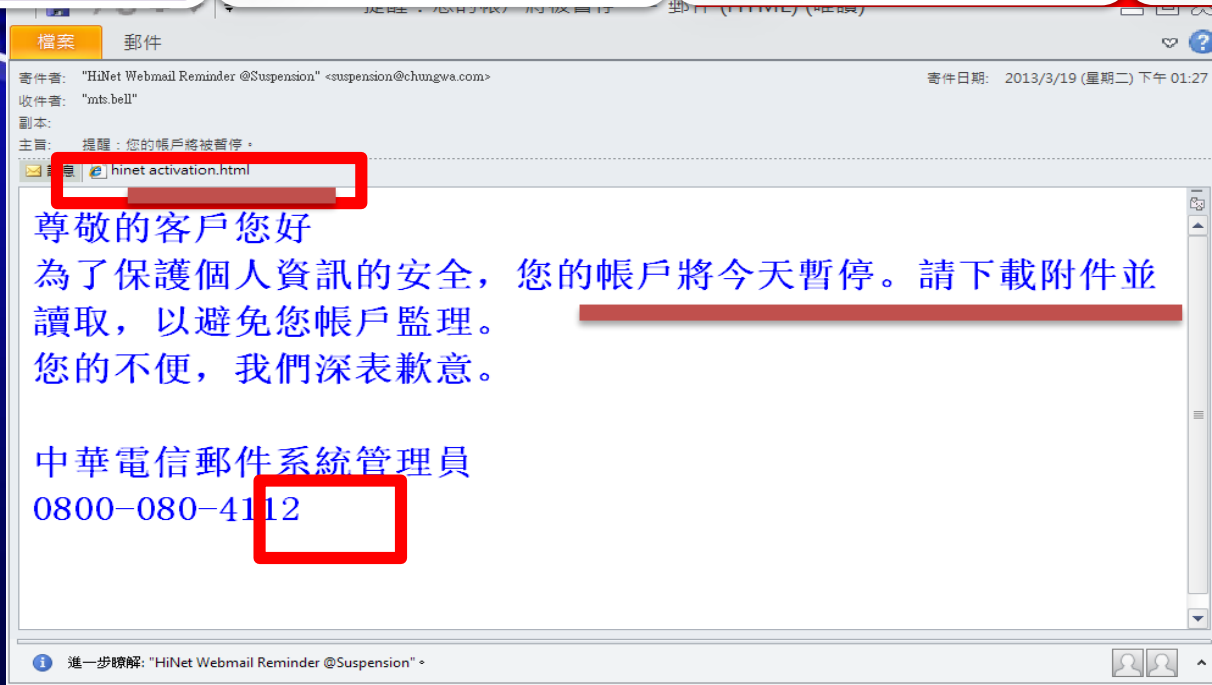
打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



某電信公司釣魚信件



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

Verify - Login x

www.math-infobatnaa.com/info/Login.php?sslchannel=true&sessionId=zIJsK81YaAir3O4ZADYej0syFDzHXH

Store Mac iPhone Watch iPad iPod iTunes Support

## Verify Apple ID

Please sign in to verify your Apple ID/iCloud Account

Please login to verify & update your Apple ID account information

### Account Verification

We occasionally require our users to verify or update their account information on file. This can be due to invalid account details, or an expired payment method.

You will be unable to use your Apple ID or make purchases until this process is completed.

Sign in to verify your Apple ID.

Apple ID

[Forgot your Apple ID?](#)

Password

[Forgot your Password?](#)

Sign In

My Apple ID

Copyright © 2015 Apple Inc All rights reserved. [Terms of Use](#) | [Privacy Policy](#) [Choose your country or region](#)

**Phishing Web**



資安問題非一日形成



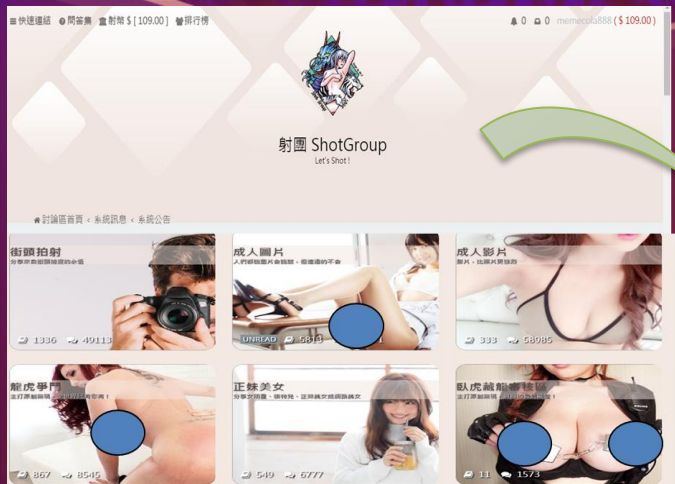
打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



# 案例4



## 豬隊友 洩漏身分





資安問題非一日形成



打擊犯罪需要新方法



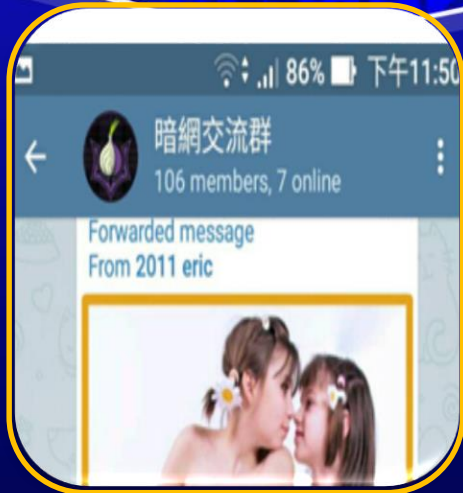
巧婦難為無米炊的困境



資安的等於國安的期望

# 案例5

使用網路嗅探



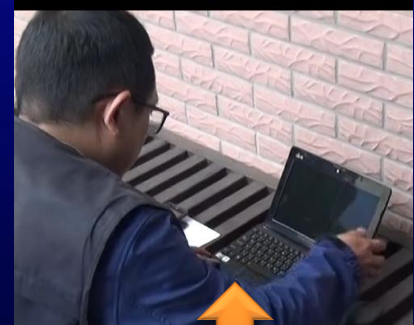
涉案社群

Telegram成立暗網幼幼圖散布群組

```
HTTP/1.1" 404 501 "-" "pyth
on/2.7.9 Windows/2008ServerR
139.162.81.62 - - [03/Aug/20
http://clientapi.ipip.net/e
HTTP/1.1" 404 470 "-" "Go-h
121.199.45.91 - - [03/Aug/20
/ HTTP/1.1" 200 11012 "http
"Mozilla/4.0 (compatible; MS
"
173.93.38.23 - - [03/Aug/201
/ HTTP/1.1" 200 10975 "-" "W
223.137.128.181 - - [03/Aug/
ET /child.jpg HTTP/1.1" 200
(Linux; Android 6.0.1; ASUS
pleWebKit/537.36 (KHTML, lik
71.125 Mobile Safari/537.36"
223.137.128.181 - - [03/Aug/
ET /favicon.ico HTTP/1.1" 40
.fortidyndns.com:8080/child.
x; Android 6.0.1; ASUS_Z00LD
Kit/537.36 (KHTML, like Geck
Mobile Safari/537.36"
223.137.128.181 - - [03/Aug/
"us u "-" "-"
27.242.107.77 - - [03/Aug/20
/child.jpg HTTP/1.1" 200 12
iPhone; CPU iPhone OS 10_3_3
bKit/603.3.8 (KHTML, like Ge
/14G60 Safari/602.1"
```

現場視視涉案人手機及電腦  
擴大追查加入群組網友及圖片來源

現場檢視手機



現場檢視電腦



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 案例6

Video player interface showing a woman in a blue jacket speaking. The video title is "台灣電信警察大隊的各位". The player includes a progress bar at 4:04 / 4:23 and various control icons. The video content shows a woman in a blue jacket speaking, with a "老天鵝娛樂" logo in the top left corner of the video frame. The video is labeled as "截取自網路" (Captured from the internet).

## 資安與色情網站犯罪打擊關聯~





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 2019迄今手機竊取簡訊又來了?



## 案例7



詐騙集團

宅配公司傳送  
不在府通知簡訊



民眾

手機內個資遭到竊取  
無法操控手機

用手機開啟追蹤貨物  
請求再次配送  
啟動惡意軟體



詐騙集團

不只偽裝宅配業者  
假冒信用卡公司



確認信用卡  
發卡狀況簡訊  
民眾千萬不要  
點開網址



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

民眾收到釣魚簡訊(內容:包裹已派發,請查收,後附網址)

民眾點選網址後於假Apple (iTunes Store)網頁

輸入自己的

密碼輸入至網

消費。

民眾收到釣魚簡訊不慎點入惡意連結,報案人門號0932XXXXX不停轉發簡訊給他人,共發出1140封簡訊,目前報案人已自行停話該門號,目前得知損失電信費用1140元

訊認證  
額付款





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 臺灣刑事局與大陸網絡安全保衛局啟動0610專案 追查出手機惡意程式散布係來自大陸



刑事局與大陸公安聯手合作，破獲首宗智慧型手機簡訊惡意程式詐欺案。警方指出，該集團2年前以「黑貓宅急便請點收」等名義的簡訊，誘騙民眾點選連接，植入木馬程式，每隔6、7秒就會回傳手機內的所有個資供不法集團犯罪，估計全台數百萬android系統用戶受到影響，詐得上千萬元。





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 一銀ATM吐鈔 指令來自倫敦分行



2016-07-19

### 分行兩電話錄音硬碟遭駭

〔記者陳慰慈、謝君臨／綜合報導〕警方前天逮捕第一銀行A T M盜領案主嫌安卓斯等三人，起出贓款六千多萬，檢調警偵辦這起國內首宗國際駭客集團盜領案又有重大進展，專案人員解析一銀電腦及A T M硬碟發現，一銀倫敦分行電腦主機內的兩個電話錄音硬碟遭駭，研判犯罪集團入侵倫敦分行主機後，遠端遙控A T M吐鈔。



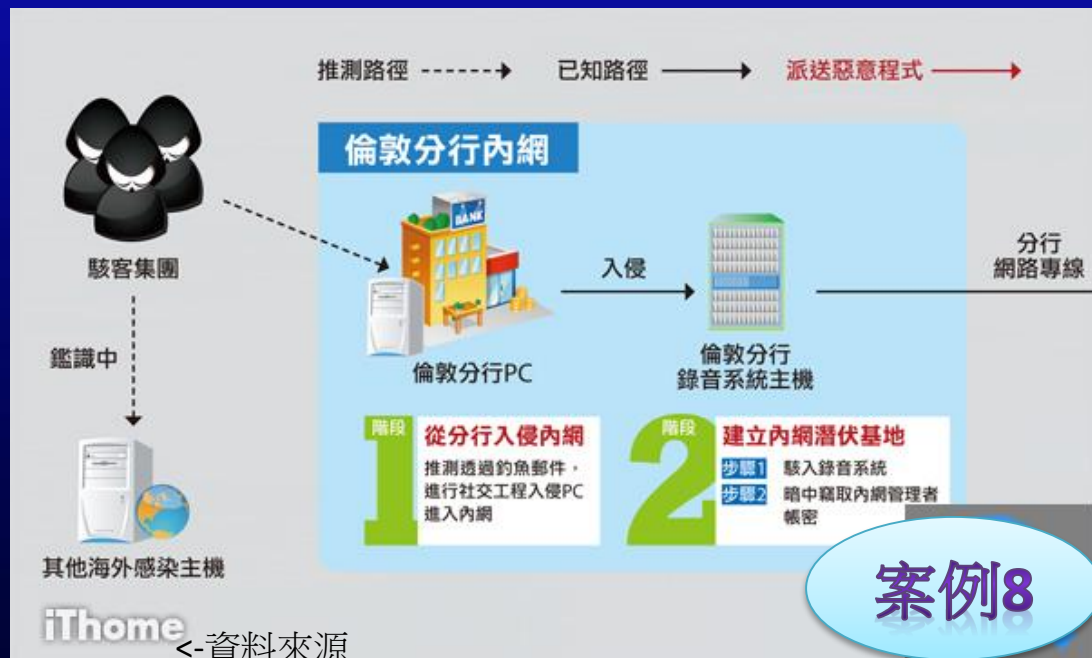
新北市調查處昨以證人身分約談一銀倫敦分行主管、資訊處主管及A T M設備廠商共三人到案，訊後請回，三人今將至台北地檢署複訊。

### 趁軟體更新植入吐鈔程式

盜領案發生後，資安調查官複製一銀與A T M連線的主機資料，以及所有被駭的A T M硬碟，送回調查局資安實驗室鑑識分析，經一週鑑識比對，確認盜領案發生的九日到十一日間，一銀倫敦分行電話錄音

主機與台灣A T M曾有異常連線，觸及到防火牆，認為倫敦分行是被駭

# 一封電子郵件破掉銀行金鐘罩



案例8



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 物聯網威脅-信用外洩管道

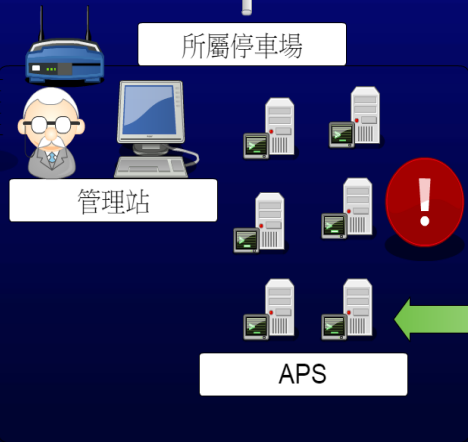
## 案例9

某停車場管理公司



某資料交換平台

所屬停車場



境外駭客



維護或外包廠商





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 駭客的社交工程(詐術演變)





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 病毒-木馬 惡意程式 範例

名稱	修改日期	類型	大小	名稱	修改日期	類型	大小
4869416-但願人長久-C調	2018/5/10 下午 06:36	捷徑	2 KB	106-1 非同步遠距教學 資訊學院 資管系 ...	2018/1/22 下午 05:31	檔案資料夾	
4869416-但願人長久-G調							
Fly_Me_To_The_Moon-C調							
Funiculi_Funicula-單音-bB調							
Funiculi_Funicula-單音-C調							
Rondo_Alla_Turca-change							
System Volume Informatio							
The_Moon_Represents_My							
The_Moon_Represents_My							
The_Moon_Represents_My							
女人花_nurenhua_meiyanfa							
女人花_nurenhua_meiyanfa							
告白氣球_Jay_Chou-bB調							
告白氣球_Jay_Chou-bE調	2018/5/10 下午 06:37	捷徑	2 KB	codevisual2flowchart.exe	2015/6/10 上午 12:41	應用程式	1,709 KB
告白氣球_Jay_Chou-C調	2018/5/10 下午 06:37	捷徑	2 KB	Wireshark-win32-1.12.13.exe	2018/7/23 下午 06:11	應用程式	23,209 KB
往事乾杯-C調	2018/5/10 下午 06:37	捷徑	2 KB	Wireshark-win32-2.6.2.exe	2018/7/23 下午 06:09	應用程式	52,979 KB
				Wireshark-win64-2.6.2.exe	2018/8/3 下午 03:33	應用程式	58,559 KB
				專題報告C組.rar	2018/3/3 下午 07:05	RAR 檔案	17,074 KB
				網站磁碟分享工具_hfs.exe	2010/7/12 上午 09:39	應用程式	560 KB

- 2017-這是你昨天被偷拍的照片嗎.rcs.jpg
- 2018-公務人員退休金\_計算辦法\_機密檔案.rcs.doc
- 2018-選舉秘辛-公投開票的秘密影片.rcs.mp3
- 2018-選舉秘辛-高票落選的秘密文件.rcs.pdf

- 2017-這是你昨天被偷拍的照片嗎.rcs.jpg
- 2018-公務人員退休金\_計算辦法\_機密檔案.rcs.doc
- 2018-選舉秘辛-公投開票的秘密影片.rcs.mp3
- 2018-選舉秘辛-高票落選的秘密文件.rcs.pdf

駭客攻擊重點:

1. 資料損壞
  2. 設備破壞
- 隨機攻擊或特定目標



資安問題非一日形成



打擊犯罪需要新方法

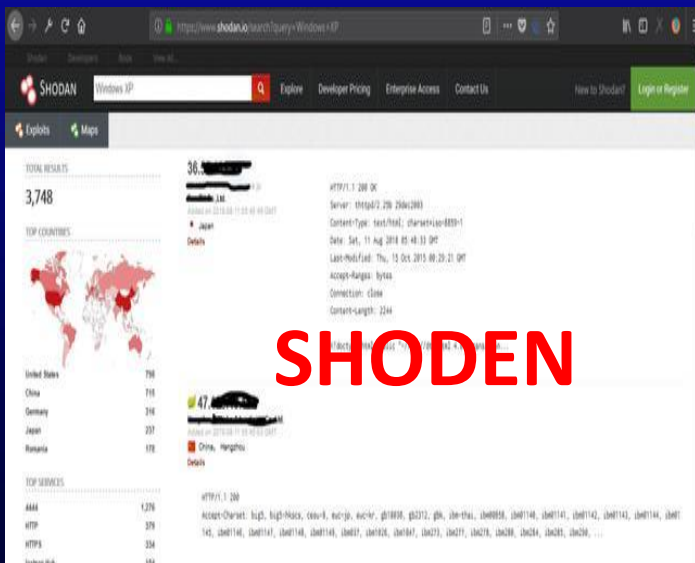


巧婦難為無米炊的困境



資安的等於國安的期望

# 第三方網站與暗網



案例 10





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

社會

社會焦點

保障人權

暗黑絲綢路／違法的..「暗網」都賣 警：各國都難抓

1g GRAM 90% Pure Cocaine



฿0.0663

£65

Veripurity420 (2350) (4.90★)

Ships to Europe

Ships from UK

Escrow Yes



▲黑市「夢想市集」上的純度90%的古柯鹼，1克的售價折合台幣約3000元。(圖／翻攝畫面)



29歲兩年狂賺77億，35歲被判終身監禁，暗網“絲綢之路”締造者絲綢之路創始人烏布里希 (Ross Ulbricht) 的末路

是暗網中最具“品牌價值”的電商，堪稱暗黑版淘寶。你能想到的東西都有可能在裡面找到。只要你情我願，就可以形成一筆買賣。毒品、性奴、兒童色情、私人殺手，下限是什麼？……



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

暗网交易论坛

用户名   自动登录  
密码   [注册帐号](#)

暗网交易论坛 会员验证激活 帮助中心&交易指南 充值(比特币)

请输入搜索内容   热搜: 银行卡料 国外护照 社工资料库 女星性爱视频 找关系办事 来钱快的工作

今日: 3015 | 昨日: 701 | 帖子: 57792 | 会员: 9309 | 欢迎新会员: 网虞礼

首页推荐

最新主题	最新回复	精华帖子	人气热门
<a href="#">山东省身份数据50W条</a> <a href="#">19年棋牌数据整合500W条</a> <a href="#">2019年跟投之家原数据</a> <a href="#">xcp89.com金利来彩票城18W综合数据</a> <a href="#">2018年下半年彩票数据18W条</a> <a href="#">澳门金沙城19年12月彩票数据</a> <a href="#">19年彩票红联系单式30条</a> <a href="#">财经网和讯网注册用2W条数据</a> <a href="#">221W全国居民基金证券数据北京中</a>	<a href="#">221W全国居民基金证券数据北京中</a> <a href="#">迪丽热巴各种视频合集</a> <a href="#">CVV刷货教学 多个徒弟 包出货</a> <a href="#">支付宝强制注册 提现账户店铺账户</a> <a href="#">出售cvv核理神器antidetec7.1</a> <a href="#">本科 研究生 教师资格证 落户北</a> <a href="#">失信人买机票高铁票</a> <a href="#">山东省身份数据50W条</a> <a href="#">221W全国居民基金证券数据北京中</a>	<a href="#">出售cvv核理神器antidetec7.1</a> <a href="#">出售山西长治美女性奴资料和调教</a> <a href="#">监听别人手机信息, 微信, qq聊天</a> <a href="#">全网最低价8500MB银行卡四件套因</a> <a href="#">迪丽热巴各种视频合集</a> <a href="#">出售台湾身份证文本信息, 另出售</a> <a href="#">手轮制图图纸 M1911-A1</a> <a href="#">最新安卓遥控手机木马源码!!</a> <a href="#">X2 芯片卡写卡软件</a>	<a href="#">国产幼 我本第一季80G 第二季100</a> <a href="#">各种折扇, 分尸视频...</a> <a href="#">甜美小姐姐, 迷晕被带到旅馆, 啪</a> <a href="#">美若天仙的9岁小姑娘陪爸爸玩</a> <a href="#">初中生, 小学生理体才艺表演</a> <a href="#">网红女神有暗器HK旅拍83P3V</a> <a href="#">好莱坞女星艳照门和一些做爱视频</a> <a href="#">多位国内女明星合成图</a> <a href="#">真人妇科检查</a>

交易市场

<b>关系人脉 (419)</b> 主题: 110, 帖数: 1万 私密版块 简介: 找关系、走门子、安排工作、监察档案、信息、工作调动、清除记录、项目承包	<b>数据资料 (480)</b> 主题: 1万, 帖数: 3万 私密版块 简介: 个人信息、社工库、各类数据资料、技术资料、情报信息等非实物类资料。	<b>器械药品 (443)</b> 主题: 8988, 帖数: 1万 私密版块 简介: 器械相关技术、图纸、物品、药品药物类交易区, 发售交易有会员等级限制。	<b>卡料信息 (412)</b> 主题: 9894, 帖数: 1万 私密版块 简介: 银行卡信息、CVV卡料信息、轨道料信息, 内部数据、帐户信息等银行相关的数据。
<b>雇佣求职区 (409)</b> 主题: 6685, 帖数: 1万	<b>身份护照 (455)</b> 主题: 9342, 帖数: 1万	<b>色情成人 (432)</b> 主题: 8974, 帖数: 1万	<b>其它黑灰产业 (485)</b> 主题: 8398, 帖数: 1万

中文暗网论坛交易市场:

<http://stsp57cle7lvkex4sgpv2vtdo4ust4tt7lrjtu6uxzcvorhzwkc5zqd.onion/>



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

黑暗網路隱憂

毒品

輕熟女染毒 竟到神秘dark web買大麻



加入IS的英籍男子胡森 (Junaid Hussain) 曾透過dark web發訊要BBC臥底記者在倫敦發動恐攻。他已在敘



加入IS的英籍男子胡森 (Junaid Hussain) 曾透過dark web發訊要BBC臥底記者在倫敦發動恐攻。他已在敘利亞被炸死。 翻攝《泰晤士報》

殺人



大陸留學生章瑩穎在美國遭殺害，警方查出嫌犯克里斯坦森 (圖) 是從「暗網」學習犯罪手法。(翻攝伊利諾伊大學警察局)

人口販運



一對德國情侶長期性侵10歲的兒子，甚至透過暗網把兒子賣給戀童癖者洩欲。(東方IC)



資安問題非一日形成



打擊犯罪需要新方法



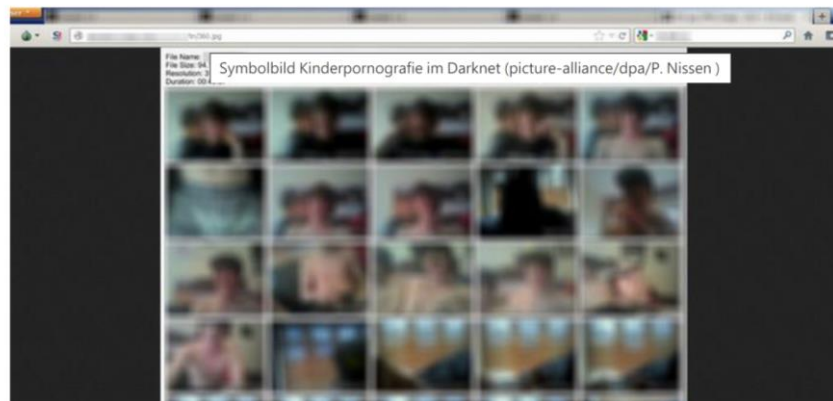
巧婦難為無米炊的困境



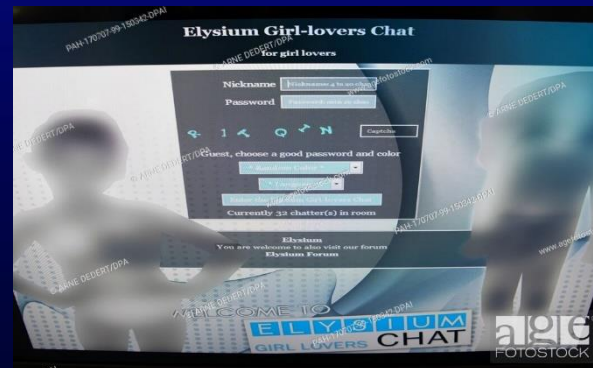
資安的等於國安的期望

## Investigators bust major darknet child porn platform

A darknet platform used by almost 90,000 members to exchange material showing children being sexually abused has been shut down, German investigators say. Most users reportedly came from Germany and Austria.



德國警察查獲  
極樂世界黑暗網路網站  
違反兒童及少年性剝削等法條  
網站架站者約39歲  
2016~2017年犯罪，約有上萬德  
國及澳大利亞會員





資安問題非一日形成



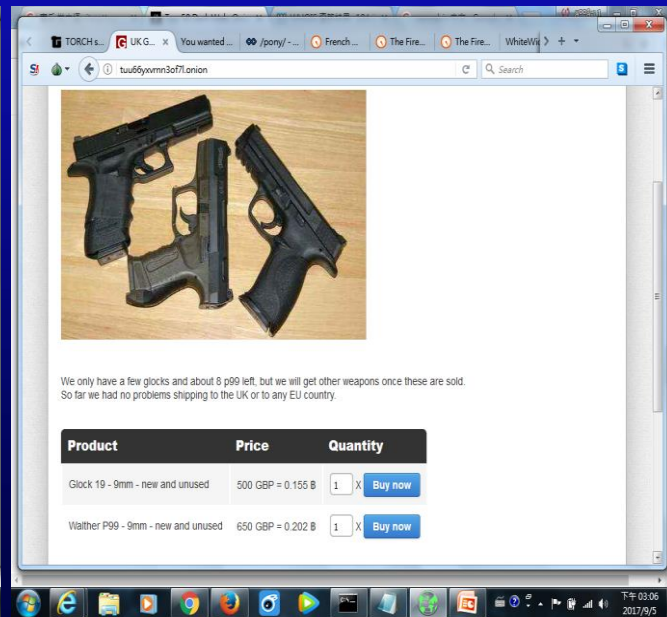
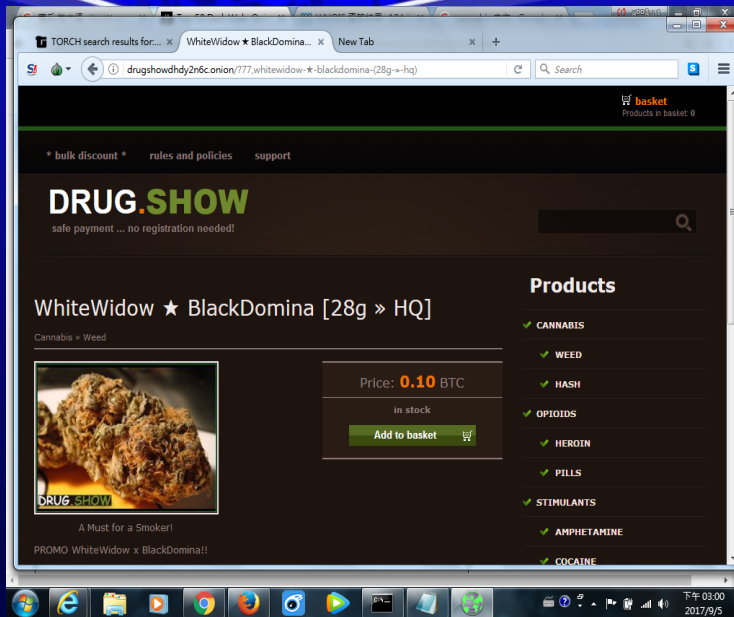
打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



販售毒品、槍枝(暗網)用比特幣交易



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 行動資料庫查詢工具

文/ 王立恆 | 2017-10-15 發表

讚 5.0 萬 按讚加入iThome粉絲團 讚 745 分享



## 資料庫運用與探勘也是非常重要的能力

<https://www.ithome.com.tw/article/117303>



資安問題非一日形成



打擊犯罪需要新方法

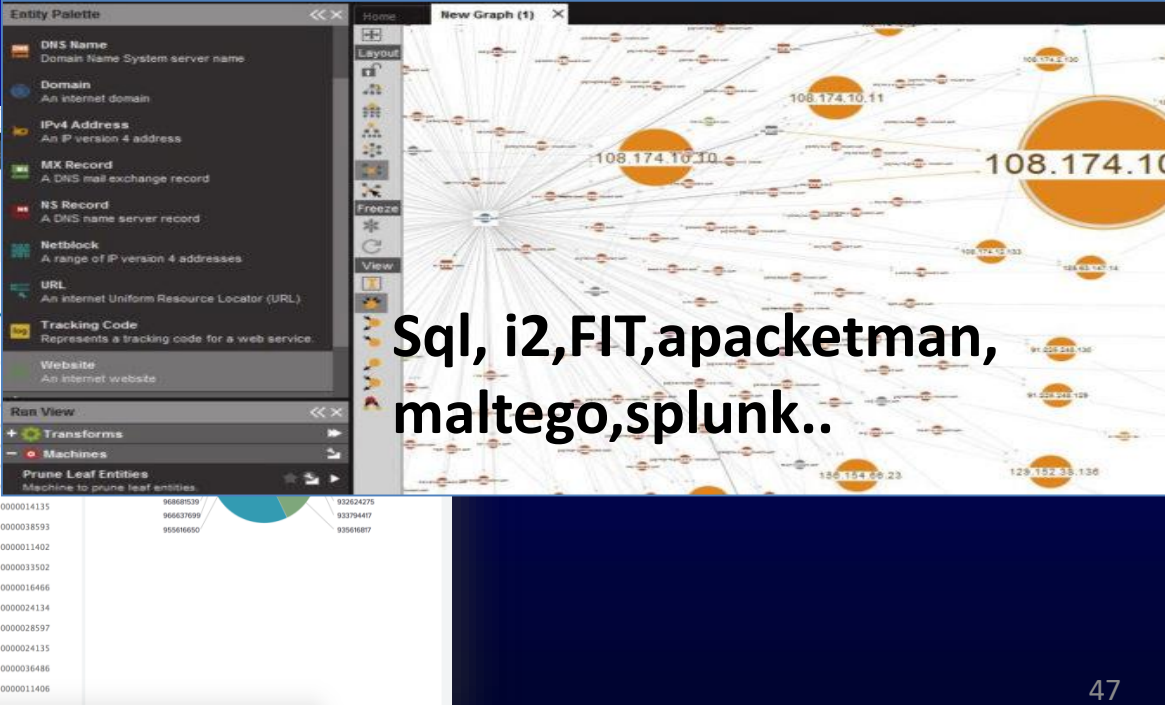
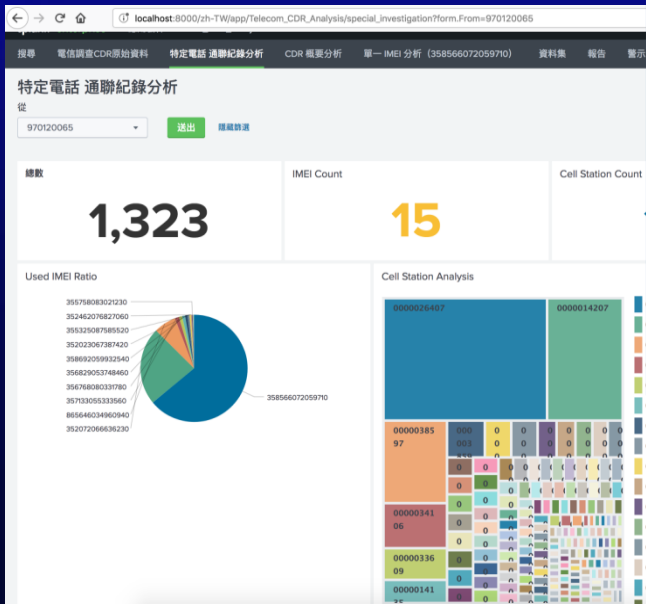


巧婦難為無米炊的困境



資安的等於國安的期望

# 資料分析工具





資安問題非一日形成



打擊犯罪需要新方法



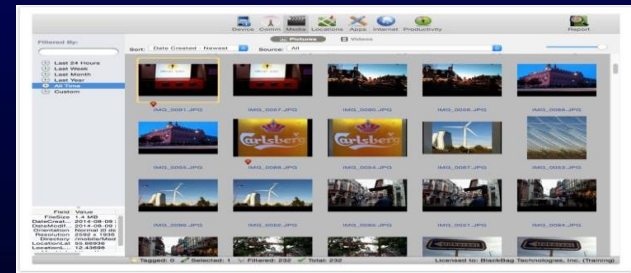
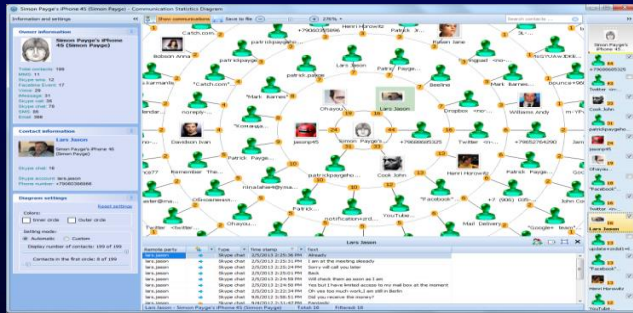
巧婦難為無米炊的困境



資安的等於國安的期望

## 數位鑑識工具(電腦、手機)

# Celebrite UFED、Oxygen、Magnet AXIOM、Mobilyze、Encase....







資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

## 異常程式運行(遠端)

時間	類別	來源	事件 ID	說明
2017/10/13 下午 01:34:01	稽核成功	Microsoft Windows security audit...	4634	登出
2017/10/13 下午 01:33:59	稽核成功	Microsoft Windows security audit...	4624	登入
2017/10/13 下午 01:33:59	稽核失敗	Microsoft Windows security audit...	5152	新運平台封包票業
2017/10/13 下午 01:33:59	稽核失敗	Microsoft Windows security audit...	5152	新運平台封包票業
2017/10/13 下午 01:33:56	稽核成功	Windows security audit...	4688	建立處理程序
2017/10/13 下午 01:33:56	稽核成功	Windows security audit...	4688	建立處理程序
2017/10/13 下午 01:33:56	稽核成功	Windows security audit...	4688	建立處理程序
2017/10/13 下午 01:33:48	稽核失敗	Windows security audit...	5152	新運平台封包票業
2017/10/13 下午 01:33:44	稽核失敗	Windows security audit...	5157	新運平台連接
2017/10/13 下午 01:33:44	稽核失敗	Windows security audit...	5152	新運平台封包票業

電腦中存在著各式各樣的資訊，如同圖書館等待偵查人員去尋寶，找到犯罪者身分...

## 事件紀錄簿V.S.該VNC程式LOG檢測



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



犯罪現場搜索



數位鑑識



雲端主機查扣





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



清查洗錢的金流，透過電磁紀錄與數位證物軌跡仍可追查犯罪所得，最後向臺地方法院聲請扣押。



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 科技設備環繞，還要有多少種鑑識出現???



- 電腦鑑識
- 週邊設備鑑識
- 雲端鑑識
- 行動載具鑑識
- 物聯網鑑識
- AI鑑識??



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

Administ

規範不斷出現，主要讓證據更客觀，講求信度，效度也不能忘

美國國家標準技術研究所(National Institute of Standards and Technology, 簡稱NIST)於2006年制定的電腦網路標準鑑識及分析程序 **NIST SP 800-86** 《Guide to Integrating Forensic Techniques into Incident Response數位鑑識技術指南》及2014年公布行動裝置鑑識準則 (Guidelines of Mobile Device Forensics, **NIST-SP-800-101 Revision 1**) 對於行動裝置鑑識程序及方式等作法，遵循下列四大步驟:收集(Collection)、鑑識(Examination)、分析(Analysis)、呈現(Reporting)步驟,美國國家標準技術研究所於2014年公布行動裝置鑑識準則 (Guidelines of Mobile Device Forensics, **NIST-SP-800-101 Revision 1**)，這準則中介紹行動裝置鑑識處理流程及方式等，其中在檢驗、分析因受限於鑑識工具所能提供的擷取方式。

**ISO17025 實驗室國際認證**，使鑑識之結果及方法流程可於國際間ISO規範下之各實驗室間相互承認。

**ISO27037**中提及，識別程序包含搜尋、辨識及記錄潛在的數位證據。識別程序應該辨識出可能存有與事件相關之數位證據的數位儲存媒體及運行的設備。

永遠追不上的技術標準規範

- 您是不是要查：資安 ISO 17025 認證
- 中華電資安實驗室獲ISO 17025認證-中時電子報  
www.chinatimes.com/realtimenews/20170323006340-260412  
2017年3月23日 - 中華電信HiNet SOC資安鑑識實驗室日前正式通過ISO 17025認證，由財團法人全國認證基金會(TAF)驗證，順利取得「資安鑑識實驗室」資格，是...
- 安審資訊通過兩項ISO 17025國際認證 | iThome  
https://www.ithome.com.tw/ipr/116042  
2017年8月3日 - 安審資訊在2005年開始提供國內政府及企業7x24小時的資安即時監控(SOC)服務，並取得國際資訊安全認證ISO27001及個人資訊管理...
- 中華電資安實驗室喜獲ISO 17025認證 產業-科技 | 中央社商情網  
cnabcbeta.cna.com.tw/news/2-03/201703231635.aspx  
2017年3月23日 - 中央社記者吳家豪台北2017年3月23日電)中華電信(2412) HiNet SOC資安鑑識實驗室日前正式通過ISO 17025認證，由財團法人全國認證基金...
- 《電腦設備》安審資訊通過兩項ISO 17025實驗室認證\_富聯網  
money-link.com.tw/RealtimeNews/NewsContent.aspx?sr=31864900010pu\_2  
2017年8月2日 - 安審資訊在2005年開始提供國內政府及企業7x24小時的資安即時監控(SOC)服務，並取得國際資訊安全認證ISO 27001及個人資訊管理...
- 資安顧問服務Security Consulting Services - 安華聯網科技-滲透測試...  
https://www.gowatpssecurity.com/service/item/32



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

# 居安思危你我都能反駁變反攻



隨時注意異常



自我檢視電腦



紀錄關鍵事件



工具運用查找



化被動為主動



防駭SOP



資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



產官學研整合，  
有效提升國內  
資安水平



建立跨體系平  
臺，加強各種  
資源交流



跨國聯防與調  
查，有效遏止  
網路組織犯罪



引進先進資安  
工具，培育優  
秀調查人才



發揮臺灣精神，  
整合強大能量  
世界發光





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望



人才培育：  
十年寒窗無人問，一舉成名天下知







資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

運氣是留給隨時準備好的人





資安問題非一日形成



打擊犯罪需要新方法



巧婦難為無米炊的困境



資安的等於國安的期望

資安就是國安？ 資訊大爆炸，對於資安是扮演資安防護者角色？警方？MIS？業者(電信、網路、設備、系統)？第三方資安？全民？



