戶籍、身分個資與國家安全

財團法人資訊工業策進會

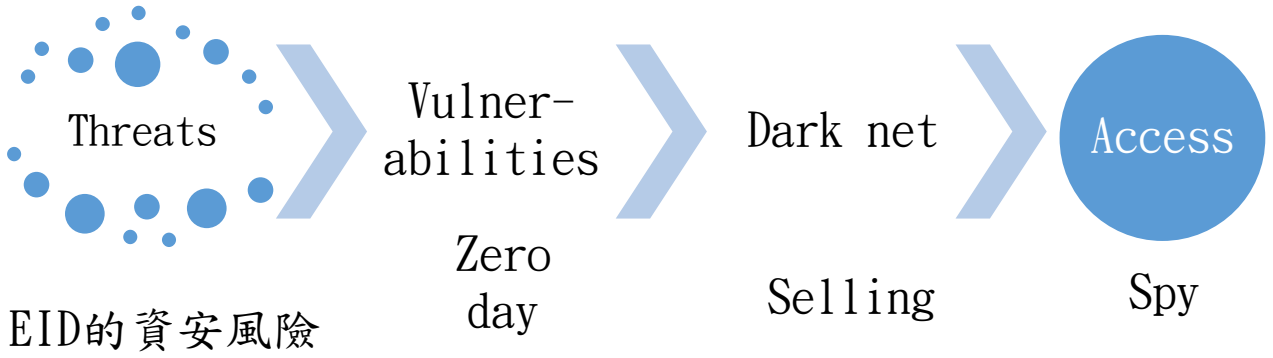
資安科技研究所 策略研究總監 王仁甫

台灣駭客協會(HITCON) 理事
TWNIC資安委員

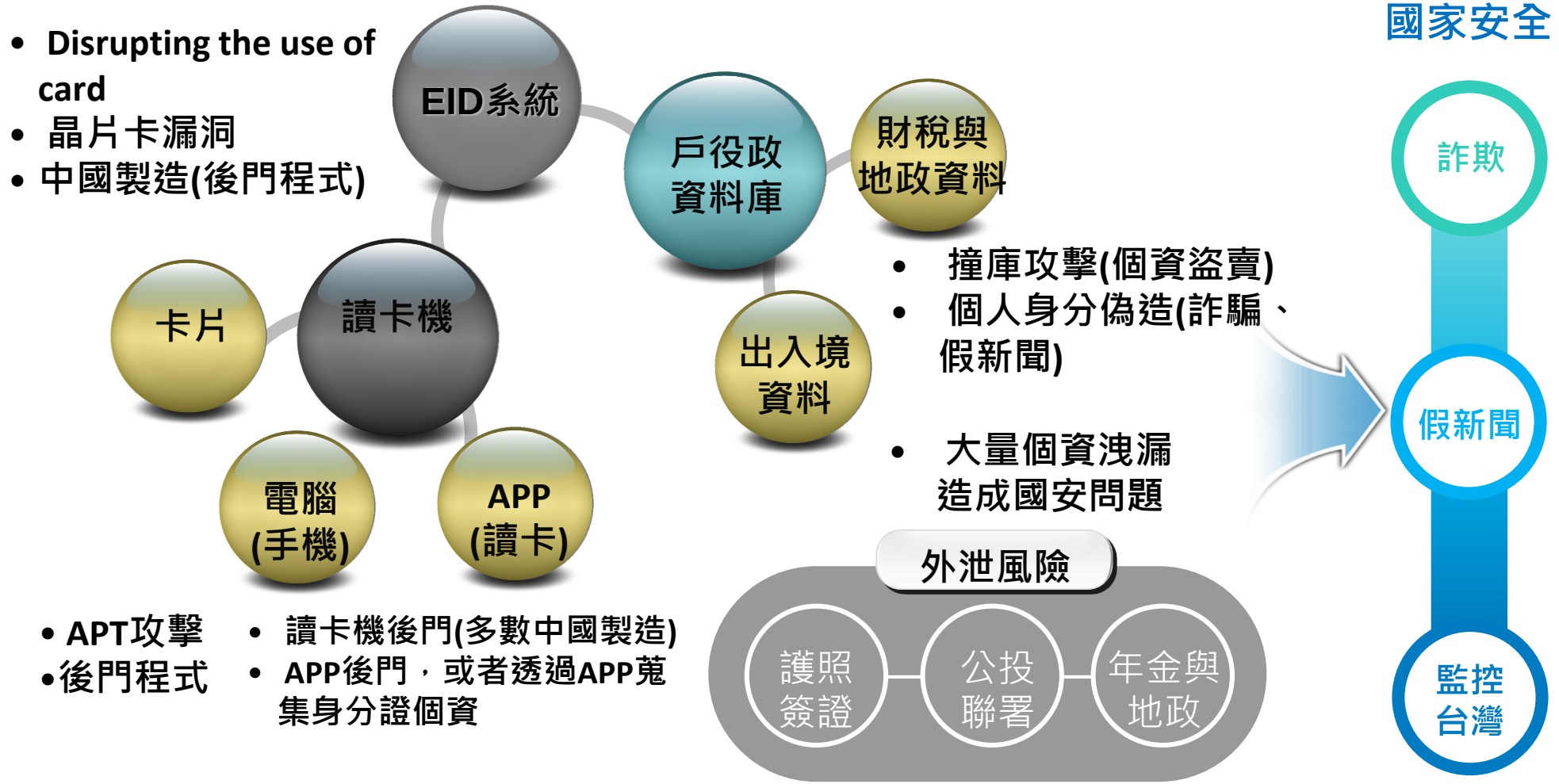
Email: jenfuwang@iii.org.tw

Outline

1. EID的資安風險
2. 身分個資洩漏與國家安全
3. 結論與建議



EID Attack Tree



Black Hat ：EID與讀卡機皆可駭

- 2008BLACK HAT 駭客 Laurie展示開發工具可以破解信用磁條、RFID，駭入EID、信用卡及護照等系統
- 2018年企業安全解決方案供應商Positive Technologies黑帽（Black Hat）駭客大會上指出，行動收銀機（mPOS）裝置含有眾多漏洞，將允許不良商家竄改螢幕上所顯示的金額，或是讓駭客取得消費者的支付卡資訊。

Vulnerabilities in mPOS devices could lead to fraud and theft

Vulnerabilities in mPOS (mobile point-of-sale) machines could allow malicious merchants to defraud customers and attackers to steal payment card data, Positive Technologies researchers have found.

Black Hat Researcher Hacks Credit Cards

Newly released tool grabs credit card account ID data off magnetic strips, RFID chips

WASHINGTON -- BLACK HAT DC 2008 -- Ever wonder what's on that magnetic strip on your credit card? Researcher Adam Laurie did, and here today at Black Hat DC he demonstrated and released a tool he developed fo hacking credit-card mag strips as well as RFID chips implanted in some card

Laurie, best known for his Rfidiot set of tools for hacking all things RFID (building passes, animal ID tags, passports, etc.), showed how his new Chap tool could find account identification data stored on a credit card. Chapy is a Python-based script Laurie wrote that works with a card reader to scan and clone the data stored on the credit card.

"I had been wondering what was on my credit card," says Laurie, whose tool for now only works with Personal Computer/Smart Card (PCSC)-based technology.

Source:https://www.helpnetsecurity.com/2018/08/10
https://www.ithome.com.tw/news/125208
https://www.darkreading.com/attacks-breaches/black-hat-researcher-hacks-credit-cards/d/d-id/1129311

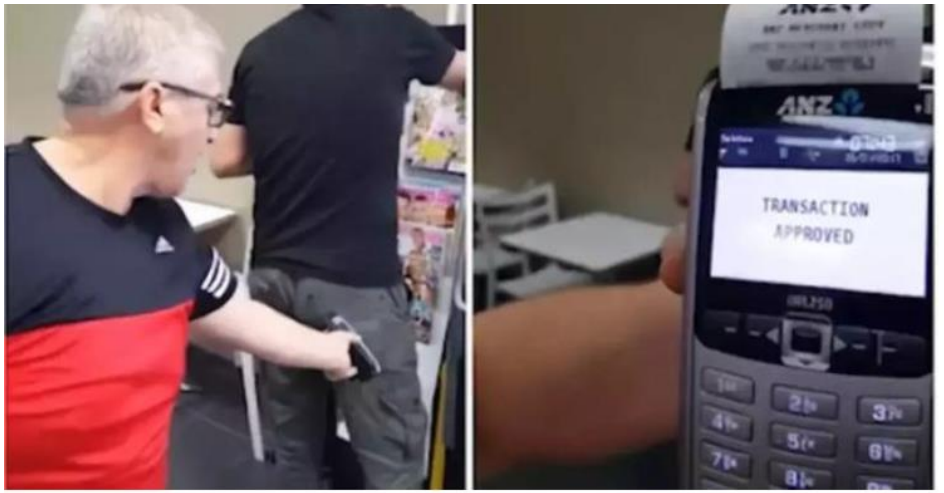
卡片終端裝置中間人攻擊

The hackers will always attack the weakest point and the weakest point is the user.

資安公司Positive揭露Visa感應式支付存在漏洞，可讓駭客進行中間人攻擊繞過支付限制，Positive已經成功在5家英國主要的銀行，實現這個感應式支付攻擊，無論使用的卡片終端裝置為何，都可以繞過感應式支付的30英鎊限制，而且研究人員發現，這種攻擊方式可能可以在英國之外的地方進行。

Researchers from Positive Technologies claim that Visa card vulnerability can bypass contactless limits

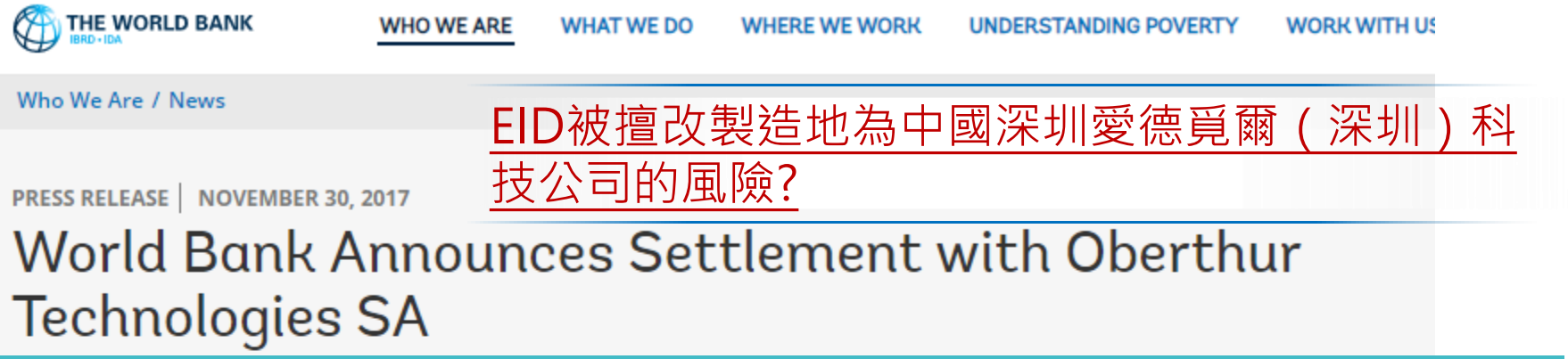
NoCash \ Cybersecurity \ Researchers from Positive Technologies claim that Visa card vulnerability can bypass contactless limits



視頻是由一個便利店老闆拍攝的，**這個短短18秒的視頻，剛上傳不到24小時便吸引了超過91萬次觀看，3萬6千多次轉發！**該店主展示了如何用一個刷卡機，輕鬆將你放在銀行的錢瞬間偷走！

資料來源:[1]李建興(2019)，資安研究人員成功繞過Visa感應式卡片支付的刷卡金額限制，ITHOME
[2]https://nocash.ro/visa-card-vulnerability-can-bypass-contactless-limits/
[3]https://kknews.cc/zh-hk/tech/gg943vy.html

台灣eID專案交給被IMF制裁的Idemia執行


THE WORLD BANK
IBRD · IDA

WHO WE ARE | WHAT WE DO | WHERE WE WORK | UNDERSTANDING POVERTY | WORK WITH US

Who We Are / News

EID被擅改製造地為中國深圳愛德覓爾（深圳）科技公司的風險?

PRESS RELEASE | NOVEMBER 30, 2017

World Bank Announces Settlement with Oberthur Technologies SA

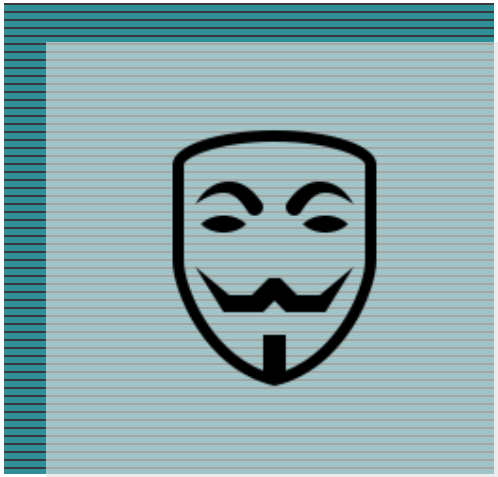
- 內政部eID標案由東元專案團隊獲得決標，3,000萬張數位身分證全部或大半，可能由國外卡廠Idemia在境外印製?
- 決定台灣New eID未來命運的Idemia是於2017年由Oberthur Technologies（OT）和Safran Identity &Security（Morpho）合併的公司 。
- 如果深入追查Idemia的前身Oberthur Technologies（OT）公司，不難發現2017年世界銀行(IMF) 官網公布制裁該公司2.5年禁令，因為其涉入孟加拉貸款1.95億美元發展eID專案的共謀貪腐、延遲履約，並擅改製造地為中國深圳愛德覓爾（深圳）科技公司 。
- 可悲的是台灣的eID專案竟然交給被IMF制裁的Idemia公司執行! Idemia公司會不會也將台灣的eID交給中國深圳子公司愛德覓爾（深圳）科技公司製造，直接將後門程式放在晶片當中?

investigation, its voluntary acknowledgment of misconduct and the

資料來源:https://www.worldbank.org/en/news/press-release/2017/11/30/world-bank-announces-settlement-with-oberthur-technologies-sa

Dark net

暗網情資販賣



暗網

威脅實例

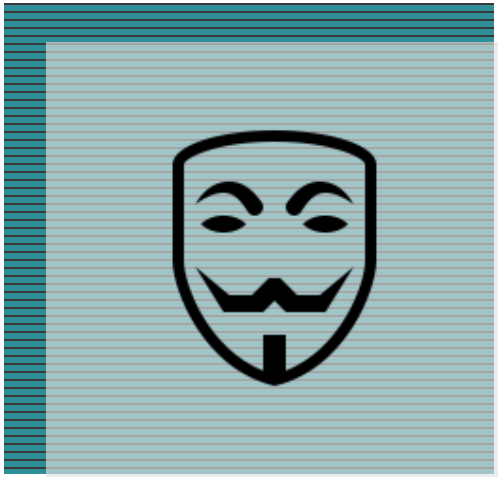
臺灣2千萬筆戶政資料暗網兜售？

2200 萬筆 Unacademy 用戶資料在暗網被出售

駭客論壇兜售3 年前 67 萬筆知名餐飲外洩顧客帳密

50 萬筆 Zoom 帳號在暗網上被販售

大量個資洩漏的風險 (1)



暗網

COVID-19影響

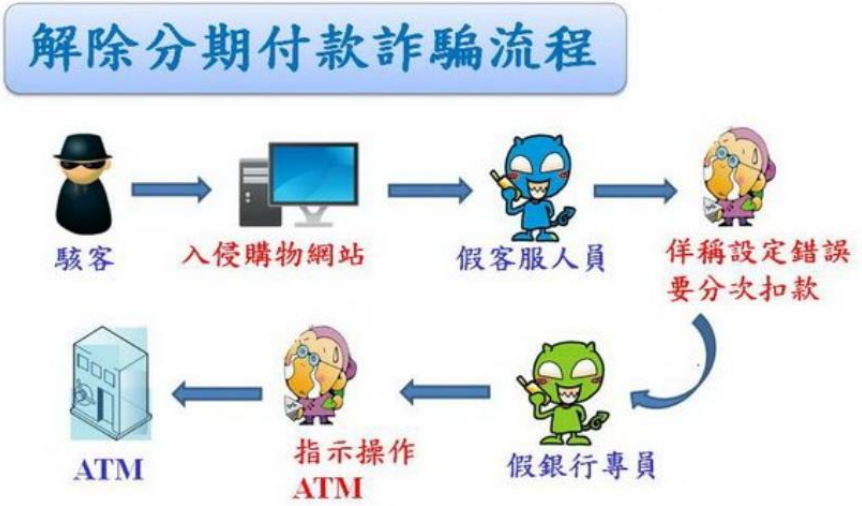
詐騙層出不窮(危及社會安全)

- **台灣電商活動普及，當詐騙公司拿到2000萬戶籍相關資料，就容易拿到家戶關係行騙，例如打給媽媽說兒子信用卡帳單逾期未繳（或者是分期付款），請媽媽去匯款解約，讓刑事局疲於奔命。**

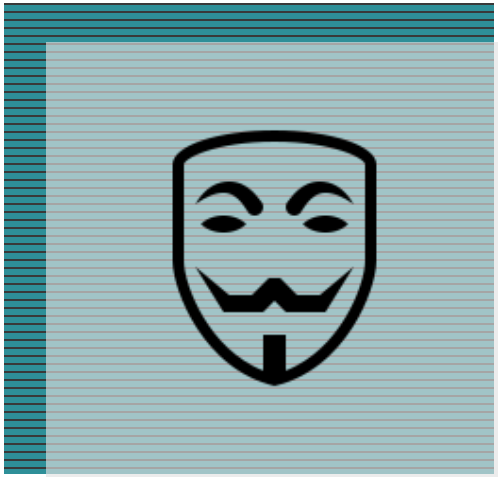
疼孫網購巧克力 遇老梗詐騙損失150多萬

中廣新聞網 | 9k 人追蹤 追蹤 2 則留言

2017年2月18日 上午10:56

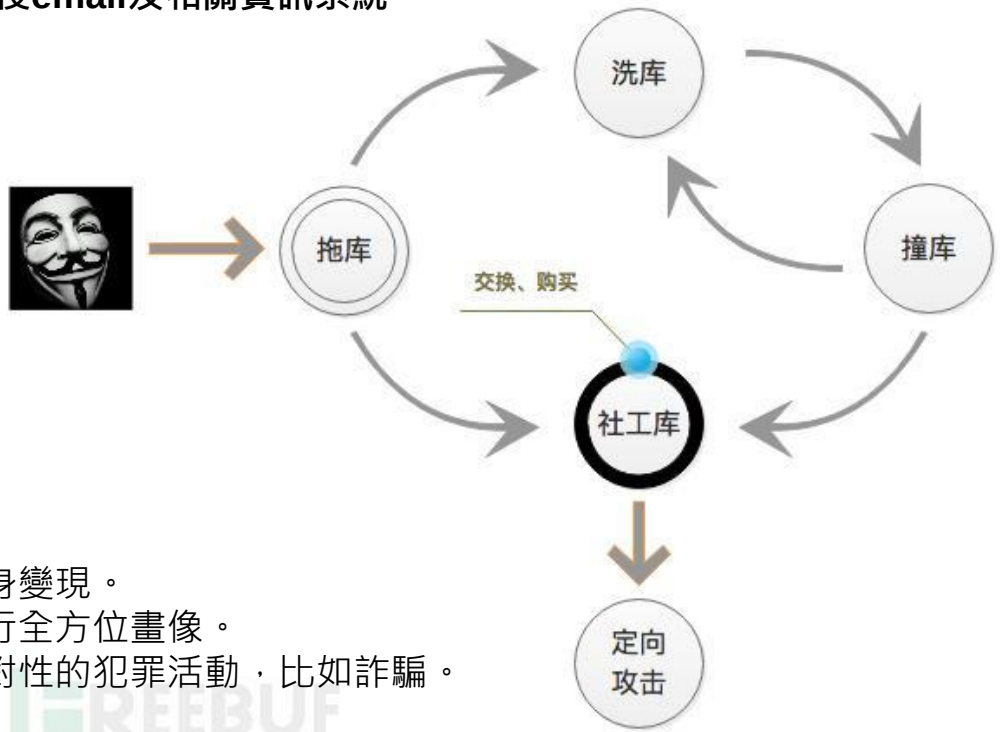


大量個資洩漏的風險 (2)



個資撞庫監控台灣人(危及國家安全)

- **人習慣用自己的個人或家人資料當成帳號密碼，最常用身分證號或生日，所以駭客集團或中共只要寫這種自動撞（資料）庫程式，就可入侵email及相關資訊系統。**

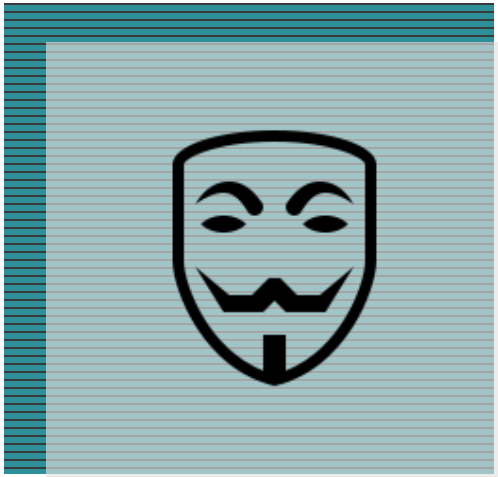


暗網

COVID-19影響

拖庫：黑客從有價值的網站盜取用戶資料數據。
洗庫：黑客將用戶賬戶的財產或虛擬財產或賬戶信息本身變現。
社工庫：黑客將獲取的各種資料庫關聯起來，對用戶進行全方位畫像。
定向攻擊：黑客根據用戶畫像，對特定人或人群進行針對性的犯罪活動，比如詐騙。
Source:https://zi.media/@yidianzixun/post/hAWGMn

大量個資洩漏的風險 (3)

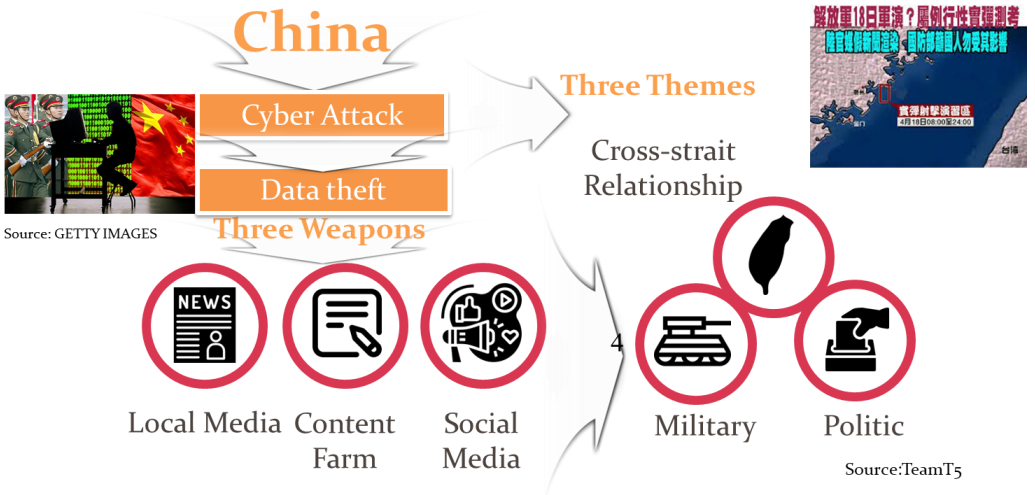


暗網

COVID-19影響

連結資料庫偽冒身分散發假新聞擾亂民主

- 只要以戶籍資料為基礎，蒐集合併個人資料，就可以掌握一個人的三大資料，包含戶籍、財務及學資歷，然後就可以在網路上偽造資料，甚至傳播假新聞（之前我們常遇到），老共找公關公司登記一堆假帳號，但登記資料特徵是台灣人，然後控制台灣民主風向。
  - Taiwan, with an advanced IT infrastructure, faces growing threat from cyberattacks, as many other highly internet-connected countries do. Taiwan faces further challenges from China, which has launched persistent attacks against Taiwanese government computer systems and targeted personnel, and engaged in disinformation campaigns.



大量個資洩漏是假新聞的禍首

中共網軍盜取台灣個資

(戰略支援部隊、國安部與公安部)

偽造意識形態行為者

公關公司炒作

酸民

EX1:Control the influx of information

Cyber Attack

Taiwan's Department of Cyber Security issued a report that there were 360 successful attacks on government systems, and 288 of these were launched by Chinese network forces.

Data theft (冒用個人身分製造假新聞)

Source:TeamT5

Three Weapons=Disinformation

- It is not necessarily to prompt the China in every article , but to reduce the negative description of China.
- In the long run, the public opinion will low the hostility to China

Content Farm

- ✓ Attracting Titles
- ✓ Contents are different from the title
- ✓ Low quality content
- ✓ Content farms created by the same person share similar style

Social Media

- ✓ High penetration rate in Facebook in Taiwan
- ✓ Mostly political articles

Local Media

- ✓ Specifically used for sharing articles to groups
- ✓ Sharing articles to its own group
- ✓ Sharing articles to other groups as soon as it is published

EX2:大量個資外洩造成的國安威脅

台灣人是中共下一個目標

- 「香港解密」網站約成立於9月左右，將個資分成3大類，分別為「毒果記者」、「港獨暴徒」、「亂港頭目」，並按姓氏分門別類。除貼出個人照片外，還洩露職業、生日、電話、臉書（Facebook）帳號、身分證及護照等個資；部分人士的住址還遭曝光。
- 所有人照片上都被蓋上「暴徒」兩字，生日、職業被曝光之外，包括台灣公民陣線發起人江旻諺和「獨眼新聞」記者Nancy兩人，連護照號碼也被公布。
- **反送中參加者及家人，除了被騷擾、黑道威脅，甚至有生命危險。**

Nancy：「香港解密把太多台灣人一個一個曝光出來，對於未來我們要入境香港，或只是轉機都有可能是一個危機。我根本不是檯面上的人，我自己被揭露出來覺得蠻詭異，也就是現在任何一個台灣人都可能是中共下一個目標。」

台人赴港反送中個資遭外洩 質疑港府幕後黑手

台灣民眾Nancy。（授權影片截圖）

人氣: 1472 【字號】 大 中 小

更新: 2019-10-23 8:36 PM 標籤: 恐嚇, Nancy, 苗博雅, 個資外洩, 香港解密

【大紀元2019年10月23日訊】立場反對反送中運動的境外網站「香港解密」，公布上百名香港抗爭者個資；還有8名支持香港反送中的台灣人，護照號碼、在香港行蹤等資料，都被公布在網站。受害者出面，質疑是港府刻意外洩資料，藉此恐嚇台灣人。

香港解密曝反送中台人個資 陸委會譴責卑劣作為

最新更新：2019/10/17 12:58

境外網站「香港解密」公布至少8名反送中台人的護照號碼等個人資料，台灣人權促進會秘書長邱伊翎（左）、基進黨主席陳奕齊（右）都遭該網站登錄。（左圖取自facebook.com/tahrfb，右圖為中央社檔案照片）

885 讚

（中央社記者繆宗翰台北16日電）境外網站「香港解密」近日公開包括基進黨主席陳奕齊在內，至少8名台人的護照號碼等個人資料。陸委會今天對此表示嚴厲譴責，並指此類卑劣作為，只會升高對立。

資料來源:https://www.epochtimes.com/b5/19/10/23/n11606612.htm

策略建議

Nancy：「香港解密把太多台灣人一個一個曝光出來，對於未來我們要入境香港，或只是轉機都有可能是一個危機。
我根本不是檯面上的人，我自己被揭露出來覺得蠻詭異，也就是現在任何一個**台灣人都可能是中共下一個目標。**」

臺灣2千萬筆戶政資料暗網兜售？

- **行政院資安處：非戶政資料，多方舊資料庫整併**
- **因應方式建議如下：**
  1. 成立暗網情蒐小組並提供持續監控服務
  2. 建立快速驗證外洩資料的機制
  3. 參考美國HIPAA 法案 ，透過法規落實醫療機構之機敏資料保護

換發無晶片ID，讓資料及政治體制，一起遠離中國

- **EID將成為中共網軍駭侵的首要目標**
- **香港反送中運動成員的個資被放到香港解密，造成生命危險**
- **EID推動後，是否成為今日香港，明日台灣**

報告完畢 敬請指教