TANet 北區資訊安全營運中心

資安案例分析

臺灣大學計算機及資訊網路中心

報告人：陳思蘊

2023年 07月 05日

03

漏洞通報與案例分析

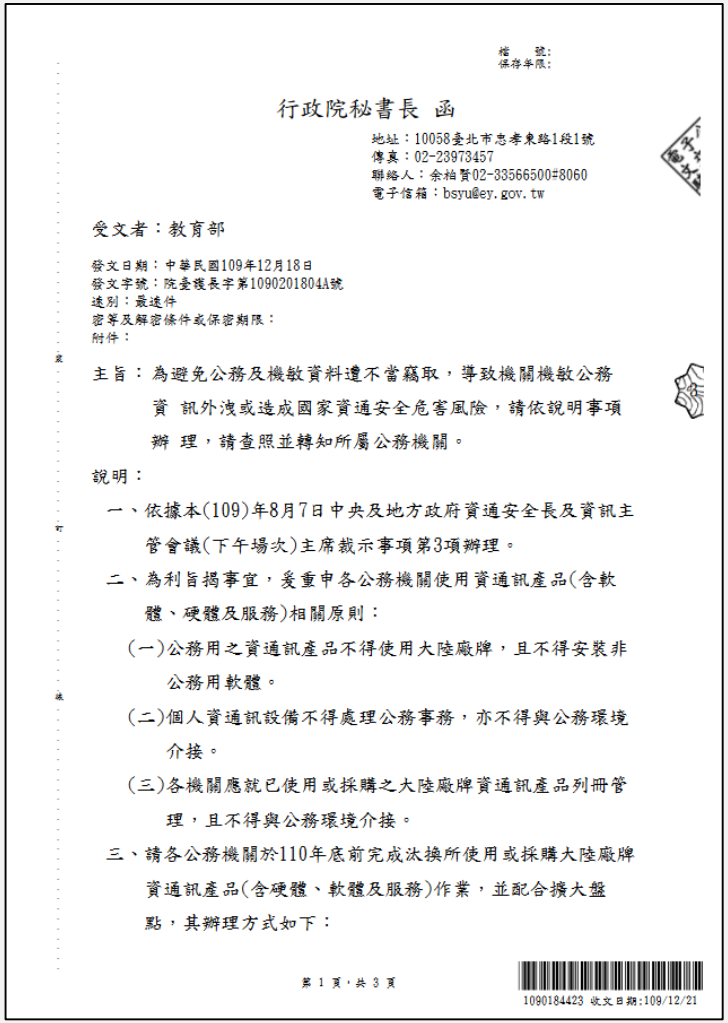
陸製設備通報(海康威視、TP-Link)
Zyxel設備漏洞通報
Mirai惡意程式與其變種
近期個資外洩案例
FTP匿名登入

大陸廠牌設備通報

TP-Link
海康威視

通報動機

- 鑑於物聯網設備應用蓬勃發展，**行政院**指示公務用之資通訊產品(含軟體、硬體及服務)**不得使用大陸廠牌**，以避免機關機敏公務資訊外洩或造成國家資通安全危害風險。
- **管理介面**暴露在**公開網路**上。



檔　號:
保存年限:

行政院秘書長　函

地址：10058臺北市忠孝東路1段1號
傳真：02-23973457
聯絡人：余柏賢02-33566500#8060
電子信箱：bsyu@ey.gov.tw

受文者：教育部

發文日期：中華民國109年12月18日
發文字號：院臺護長字第1090201804A號
速別：最速件
密等及解密條件或保密期限：
附件：

主旨：為避免公務及機敏資料遭不當竊取，導致機關機敏公務資　訊外洩或造成國家資通安全危害風險，請依說明事項辦　理，請查照並轉知所屬公務機關。

說明：

一、依據本(109)年8月7日中央及地方政府資通安全長及資訊主管會議(下午場次)主席裁示事項第3項辦理。

二、為利旨揭事宜，爰重申各公務機關使用資通訊產品(含軟體、硬體及服務)相關原則：

(一)公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。

(二)個人資通訊設備不得處理公務事務，亦不得與公務環境介接。

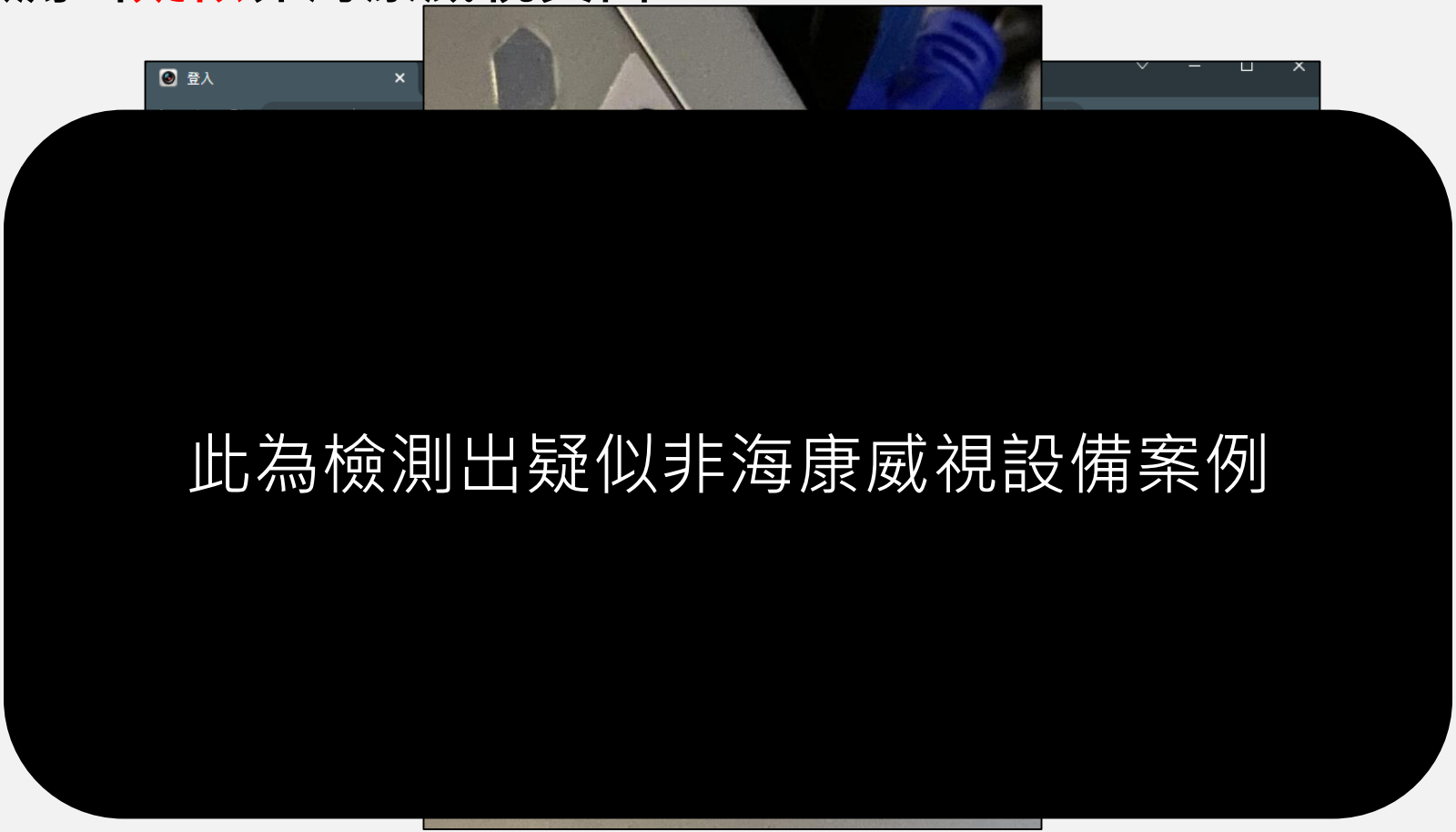
(三)各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

三、請各公務機關於110年底前完成汰換所使用或採購大陸廠牌資通訊產品(含硬體、軟體及服務)作業，並配合擴大盤點，其辦理方式如下：

第 1 頁，共 3 頁

1090184423 收文日期:109/12/21

檢測出疑似非海康威視頁面



圖片來源:https://www.cw.com.tw/graphics/surveillance-and-security-2022/

大陸廠牌設備與臺灣廠牌設備

7大證據揭露：MIT主機是中國製貼牌

台灣Benelink、中國海康監視器主機拆機實測

天下雜誌 CommonWealth Magazine

BENELINK　HIKVISION 海康威視

Benelink | 海康威視

```
<?xml version="1.0" encoding="UTF-8" ?>
<DeviceInfo version="1.0" xmlns="http://www.std-cgi.com/ver20/XMLSchema">
  <deviceName> Embedded Net DVR </deviceName>
  <deviceID> [redacted] </deviceID>
  <model>DFT6016E </model>
  <serialNumber> [redacted] </serialNumber>
  <macAddress> [redacted] </macAddress>
  <firmwareVersion>V4.21.002 </firmwareVersion>
  <firmwareReleasedDate>build 191230 </firmwareReleasedDate>
  <encoderVersion> V5.0 </encoderVersion>
  <encoderReleasedDate>build 191120 </encoderReleasedDate>
  <deviceType> IPC </deviceType>
  <telecontrolID> 255 </telecontrolID>
  <hardwareVersion> 0×20e4400 </hardwareVersion>
</DeviceInfo>
```

Benelink | **海康威視**

```
<?xml version="1.0" encoding="UTF-8" ?>
<DeviceInfo version="1.0" xmlns="http://www.hikvision.com/ver20/XMLSchema">
  <deviceName> Embedded Net DVR </deviceName>
  <deviceID> [redacted] </deviceID>
  <model>DS-7216HQHI-K1/E </model>
  <serialNumber> [redacted] </serialNumber>
  <macAddress> [redacted] </macAddress>
  <firmwareVersion>V4.21.120 </firmwareVersion>
  <firmwareReleasedDate>build 210408 </firmwareReleasedDate>
  <encoderVersion> V5.0 </encoderVersion>
  <encoderReleasedDate>build 200727 </encoderReleasedDate>
  <deviceType> IPC </deviceType>
  <telecontrolID> 255 </telecontrolID>
  <hardwareVersion> 0×20e4400 </hardwareVersion>
</DeviceInfo>
```

- Benelink的生產公司欣永成承認是海思晶片，但表示抹去晶片logo、序號是海康產品常規，與公司無關

圖片來源:https://www.cw.com.tw/article/5122864

Zyxel設備漏洞通報

CVE-2023-28771

研究動機

- CVE-2023-28771，CVSS評分高達 **9.8**分。

圖片來源：https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10442
https://www.ithome.com.tw/news/157129

Zyxel設備漏洞

- 未經身分驗證的遠程攻擊者透過發送特製的惡意UDP封包。
- 成功利用漏洞可取得root權限來執行任意程式碼(RCE)。
- 即使沒有開啟VPN服務也會遭受惡意攻擊。
- 本次漏洞發生於網際網路金鑰交換(IKEv2，Internet Key Exchange)封包解密元件。
- 48 字元(bytes)後的bytes不會被修改，以此來植入惡意反向shell(前48 bytes用來作DES解密)讓WAN介面上的500 Port(IPSec協定)回應 。

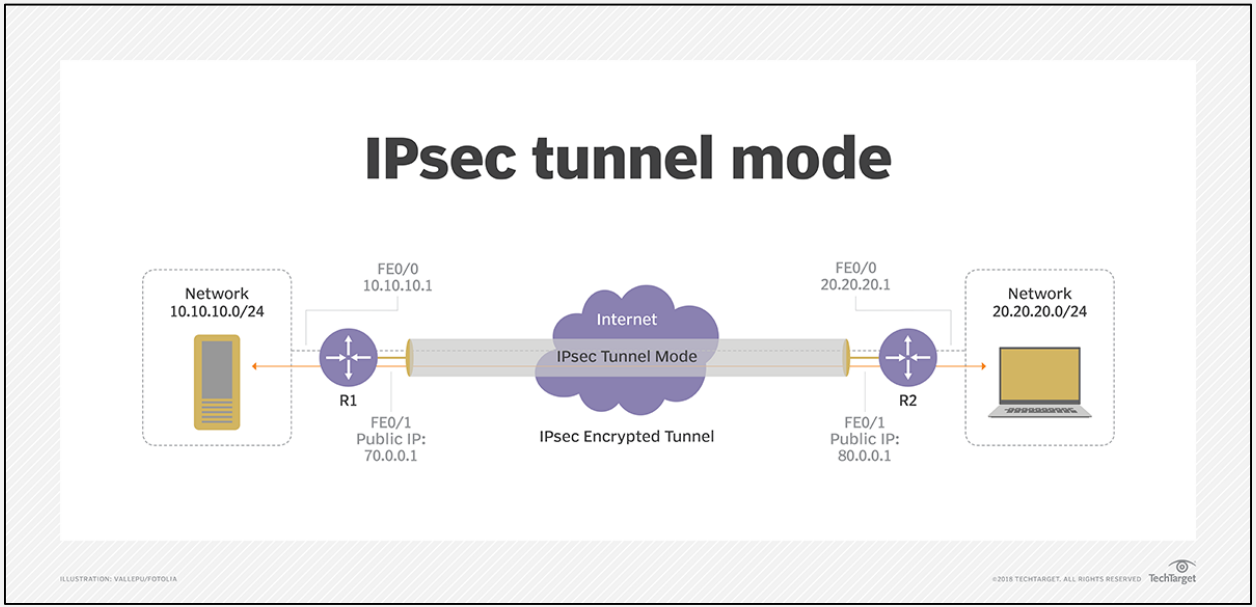
```
packet = IP(dst = args.rhost) / UDP(dport = 500) / IKEv2(init_SPI = RandString(8),
next_payload = 'Notify', exch_type = 'IKE_SA_INIT', flags='Initiator') /
IKEv2_payload_Notify(next_payload = 'Nonce', type = 14, load =
"HAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXBHAXB" + cmd) / IKEv2_payload_Nonce(
next_payload = 'None', load = RandString(68))
```

惡意封包(PoC)

參考網址：https://attackerkb.com/topics/N3i8dxpFKS/cve-2023-28771/rapid7-analysis
https://github.com/BenHays142/CVE-2023-28771-PoC/blob/main/CVE-2023-28771-poc.py#L19

網際網路金鑰交換(IKE)

- 透過虛擬私人網路(VPN，Virtual Private Network)建立雙方間安全且經過身分驗證的通訊通道。



參考網址：https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange

建議與結論

- 避免將設備的**管理介面**暴露於**公開網路**上。
- 採購設備時應請廠商協助檢視組態設定是否符合資安要求。
- 採購設備時應請廠商修補已知的漏洞。
- 定期執行設置檔備份與更新韌體。

Mirai惡意程式與其變種

Mirai 惡意程式介紹

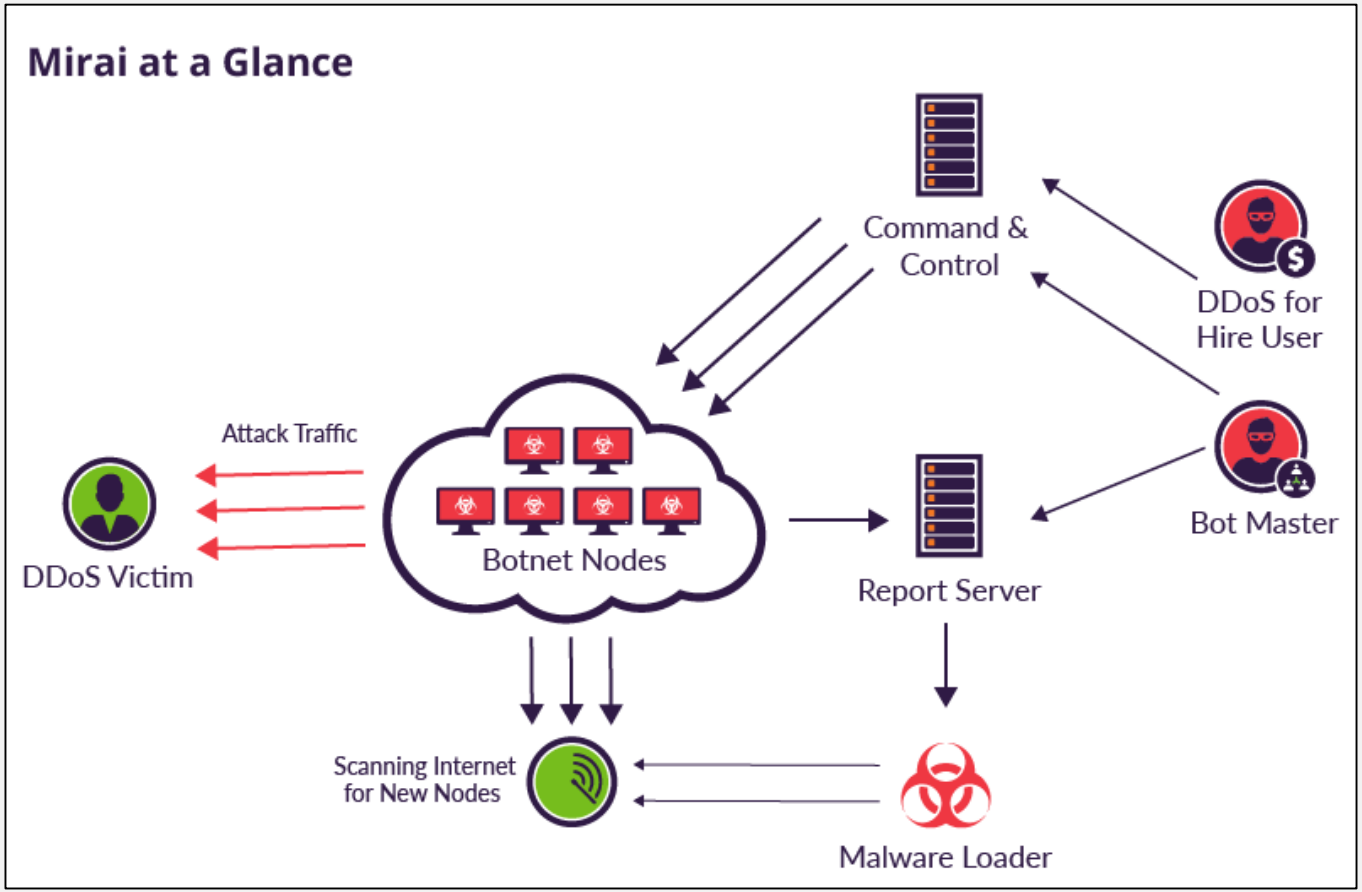
- 原先以Telnet掃描開放的Port與基於字典檔的方式暴力破解後植入惡意程式。
- 目前多個變種針對各種資安漏洞作攻擊，使其成為**殭屍網路**的一員。
- 透過大量的殭屍網路進行大規模的**DDoS攻擊**或發送垃圾郵件。
- 原始碼以**開源**的形式發布到駭客論壇，其技術亦被其他惡意軟體採用。
- GithHub內以學術研究IoT設備為由轉載的**開源程式碼**。
- 2016年幾次影響廣泛的大型DDoS攻擊均與他有關：
  - 2016/09/20 針對電腦安全撰稿人Brian Krebs的個人網站進行攻擊，攻擊量高峰達到 **620 Gbps**。
  - 2016/10/21 Dyn公司DNS服務亦遭受多次攻擊，使數個知名網站無法正常瀏覽。

參考網址:
https://zh.wikipedia.org/zh-tw/Mirai_(%E6%81%B6%E6%84%8F%E8%BD%AF%E4%BB%B6)

Mirai 的變種惡意程式

- Mirai變體繁多，僅列幾項出名的如下：
  - Asher(以Telnet暴力攻擊散播以及針對設備漏洞為目標，其中也有利用MVPower DVR漏洞)
  - OMNI (針對設備漏洞為目標，其中也有利用MVPower DVR漏洞)
  - V3G4(鎖定Linux Server、IoT設備漏洞為目標)
  - Mirai OMG(與原始Mirai相同以Telnet暴力攻擊散播)
  - Satori(鎖定IoT設備漏洞為目標)
  - Mukashi(鎖定NAS設備漏洞為目標)
  - SORA (以Telnet暴力攻擊散播以及針對設備漏洞為目標)
  - UNSTABLE(針對設備漏洞為目標)
  - Mukashi(以Telnet暴力攻擊散播以及針對設備漏洞為目標)

Mirai 惡意程式行為



參考網址:https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

建議措施與結論

- 任何設備的管理介面應放置於內部網路。
- 設備若有公開的必要請設定ACL存取清單(指定IP和Port)。
- 建議更換任何來歷不明的設備，採購設備時選擇優良廠商。
- 採購合約可要求廠商修補設備內已知的漏洞。
- 使用新設備時請新建帳號、設定高強度的密碼，並停用預設帳號。
- 定期檢視韌體或軟體是否需要更新。

近期個資外洩案例

案例分析動機

Yahoo奇摩運動
電子發票平台 資安出漏洞
公部門資安漏洞再添一樁，時代力量立委邱顯智昨天說，財政部「電子發票整合服務平台」出現重大漏洞，使用財政部發給預設密碼的事...
4 天前

鏡週刊
電子發票平台資安爆漏洞 逾 7% 上市櫃公司營業陽私恐外洩
臺灣公部門再傳資訊安
名單，指稱財政部負責
2 週前

風傳媒
財政部「電子發
「會員資料恐被
台灣公部門又傳資安疑
安缺失，只要輸入企業
2 週前

上報Up Media
電子發票平台爆
善密碼弱點--上
國內資安事件頻傳！近
業統編、政府提供之預
2 週前

中國時報
教育局新生入學網洩個資 議員憂遭詐騙集團利用
台北市國中小上周公告入學資訊，國民黨台北市議員楊植斗發現，台北市政府教育局的「台北市國民小學新生入學資訊網」個資外洩，他擔憂，詐騙集團囂張，...
2 週前

台視新聞網
全被看光光！ 北市新生入學網
5月是國民小學分發入學的時候，不過最近
有資安漏洞。一旦家長驗證登入，更改就學
2 週前

自由時報
北市國小入學網竟可查學童個
台北市教育局在上周公告國中小入學資訊，
孩童就學編號稍微修改，結果卻查到其他孩
2 週前

Yahoo奇摩新聞
看光光！北市新生入學網頁個
教育局緊急關閉
台北市議員楊植斗15日在臉書上表示，5月
家長發現，驗證網站後，修改就學編號，
2 週前

鏡週刊
涉個資外洩數位部調查結果出爐 蝦皮遭罰20萬
近期有民眾在誠品網路書店購買《阿共打來怎麼辦》一書，卻接到
話提統戰議題，民眾質疑誠品個資外洩，數位部今（30）日指出，
1 小時前

自由財經
誠品個資外洩案 數位部開罰10萬元
記者徐子芩／台北報導〕有讀者在誠品網購書籍後個資被外洩，資
話，外界關注主管機關調查進度，數位發展部今（30日）表示，誠
16 小時前

Yahoo奇摩新聞
買《阿共打來怎麼辦》接統戰電話！數位部開
因涉洩個資挨罰
近日個資外洩事件頻傳，本月有民眾在誠品網路書店購買《阿共打
竟接到「統戰市調」電話，質疑誠品個資外洩；至於蝦皮、旋轉拍
15 小時前

公視新聞網
涉外洩消費者個資 數位部罰蝦皮20萬、誠品10
網 PNN
誠品生活及蝦皮等業者涉及消費者個資外洩，數位發展部日前進行
改正，今（30）日做出行政處分，開罰誠品生活10萬元罰鍰；蝦皮
15 小時前

聯合報
近3個月4萬筆個資外
詐騙猖獗，統聯客運12日發現
區監理所初步調查出爐，確定
1 週前

自由時報
駭客攻擊逾4萬筆個資
票
統聯客運5月12日發現個資外
防性暫時關閉」網路及APP訂
1 週前

公視新聞網
統聯客運疑外洩個資
PNN
統聯客運發生疑似個資外洩案件，有民眾接到電話，被告知「誤訂大量車票」，而且個資都被對方掌握。公路總局表示，將要求業者進行調查，2天內會有初步...
2 週前

ETtoday
疑個資外洩！統聯旅客遭詐騙存款剩92元 訂票系統開放無時程表
統聯客運資料庫疑遭駭，傳出部分旅客接獲詐騙，甚至有學生反應存款都被騙了，只剩下92元，統聯緊急關閉訂票系統，進行資安調查，迄今仍未開放，統聯...
2 週前

鏡週刊
YouBike個資外
高補償2萬
北市交通局19日曾發出
員資料外洩，事後調查
4 天前

聯合報
YouBike微笑單
針對微笑單車官方網路
證卡號與騎乘紀錄外流
4 天前

生活 - 中時新聞網
YouBike遭駭4萬
YouBike日前爆發個資
26日提出補償方案與資
4 天前

NOWnews今日新聞
YouBike個資外洩！補償方案出爐：每人500元騎乘券「這時間」啟用
YouBike日前爆發個資外洩事件，全國超過4萬人個資被外流，微笑單車今（26）日下午公布補償方案，將提供相關會員每人500元的YouBike 2.0 騎乘券，...
4 天前

YouBike

Yahoo奇摩新聞
NCC網站被爆洩個資 鄭文燦：若違法將開罰
（中央社記者賴于榛台北25日電）國家通訊傳播委員會網站被爆洩漏個資，今天上午改善完成。行政院副院長鄭文燦表示，將徹查此事，如果違反資安法，...
5 天前

Rti 中央廣播電臺
NCC網站被爆洩個資鄭文燦：徹查違法就裁罰- Rti央廣
國家通訊傳播委員會(NCC)網站被爆出洩漏民眾個資，NCC於今天(25日)上午改善完成，行政院副院長鄭文燦今天表示，將徹查此事，如果違反資安法，...
5 天前

聯合報
NCC遭踢爆洩漏個資突改系統 徐巧芯直呼：真的有這件事
國民黨北市議員徐巧芯昨晚開直播，踢爆NCC系統漏洞，只要取得一組報單號碼就能登入系統，更改末兩碼，就可以看到所有曾經申請報關者的個資。
6 天前

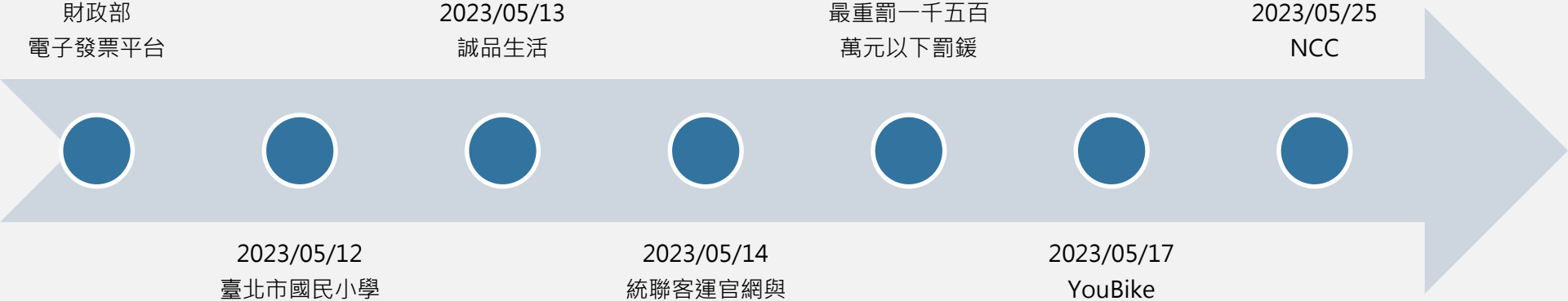
NOWnews今日新聞
遭爆網站洩漏國人個資 NCC：已加強網站身分檢核功能
國民黨台北市議員徐巧芯今（25）日指出，目前台灣購買國外3C產品只要有Wifi或藍芽等，就要到NCC（國家通訊傳播委員會）網站，上傳文件報關並填寫申請...
6 天前

NCC

統聯客運

圖片來源：Google新聞

近期個資外洩時間軸


2023/05/09
財政部
電子發票平台
2023/05/12
臺北市國民小學
新生入學資訊網
2023/05/13
誠品生活
2023/05/14
統聯客運官網與
APP
2023/05/16
立院三讀通過
非公務機關者違
法外洩個資
最重罰一千五百
萬元以下罰鍰
2023/05/17
YouBike
2023/05/25
NCC

近期資料外洩數量

時間	單位	資料外洩	備註	罰鍰
2023/05/09	財政部 電子發票平台	公司名稱、往來廠商的發票與金額	帳號密碼預設為同一組	數發布提出改善專案報告
2023/05/12	臺北市國民小學新生入學資訊網	學生姓名、戶籍地址、設籍學校與設籍日期	變更就學編號可看到他人個資	
2023/05/13	誠品生活	姓名、電話、購書清單		10萬元
2023/05/14	統聯客運官網與APP	姓名、身分證字號、生日與電話		
2023/05/17	YouBike	姓名、電話、騎乘紀錄與電子票證卡號	遭駭客入侵 發放每個會員500元騎乘券	
2023/05/25	NCC 申報進口貨品網站	姓名、電話、身分證字號、地址	輸入報單號碼更改其尾號，便可看到其他人填的資料	
蝦皮		姓名、電話、消費資料與付款方式		20萬元

個資法修法三讀通過

- 立法院於 112年5月16日三讀通過「個人資料保護法第一條之一、第四十八條、第五十六條」修正草案，修正重點整理如下：

原	修正後
中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣**二萬元以上二十萬元以下**罰鍰。	中央目的事業主管機關或地方政府可直接裁處新臺幣**2萬元至200萬元**罰鍰，毋須先限期命其改正；屆期未改正或情節重大者，罰鍰則可提高至新臺幣**15萬元至1,500萬元**。
個資法並未設置單一專責機關，由國家發展委員會(國發會)擔任個資法解釋機關。	建立個資保護獨立監督機制，由**個人資料保護委員會擔任個資法**的主管機關，整合目前分屬於中央目的事業主管機關、地方政府及國發會的權責。 最快可於8月份設立。

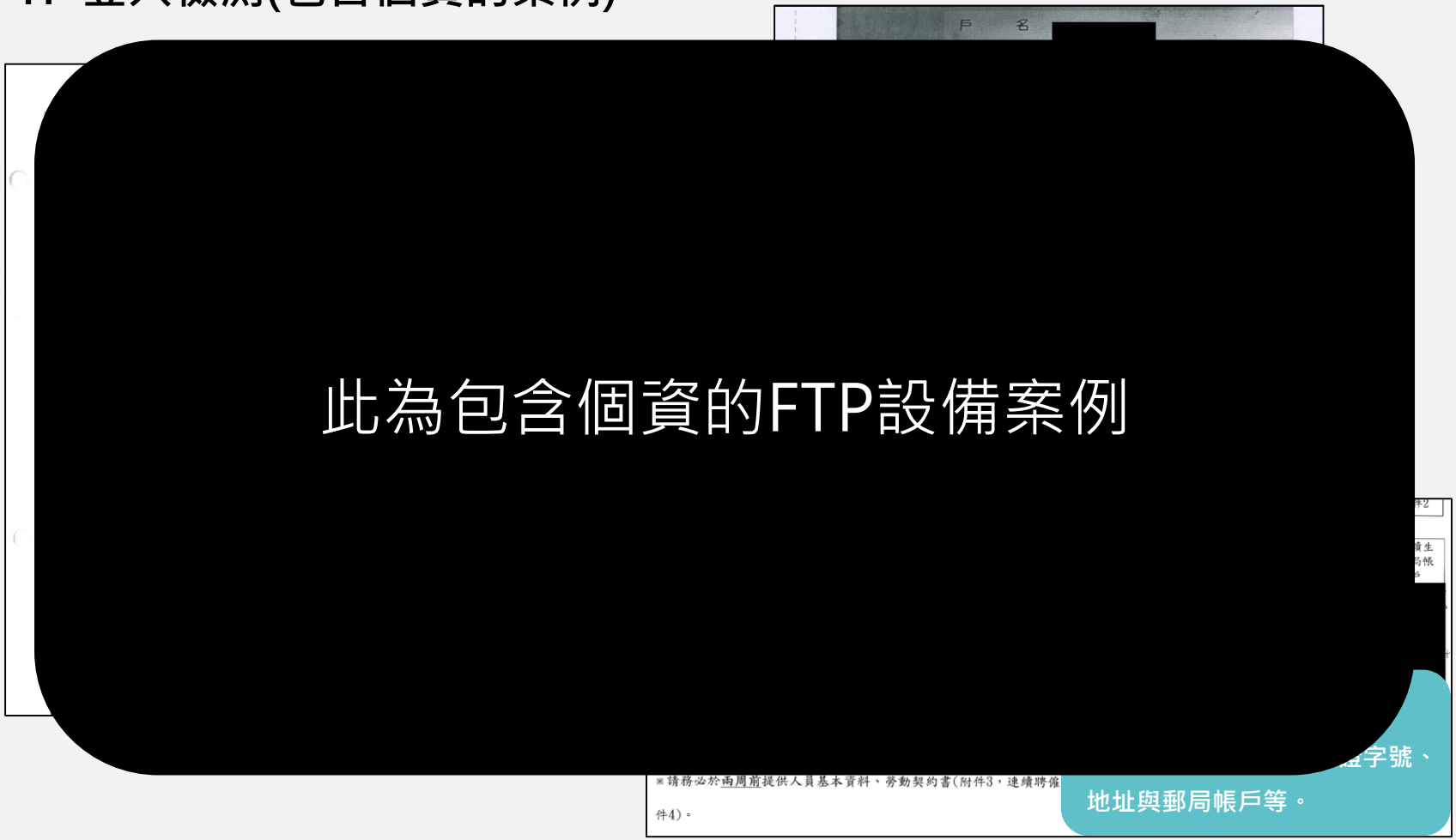
參考網址：https://www.ndc.gov.tw/nc_27_36901

建議與結論

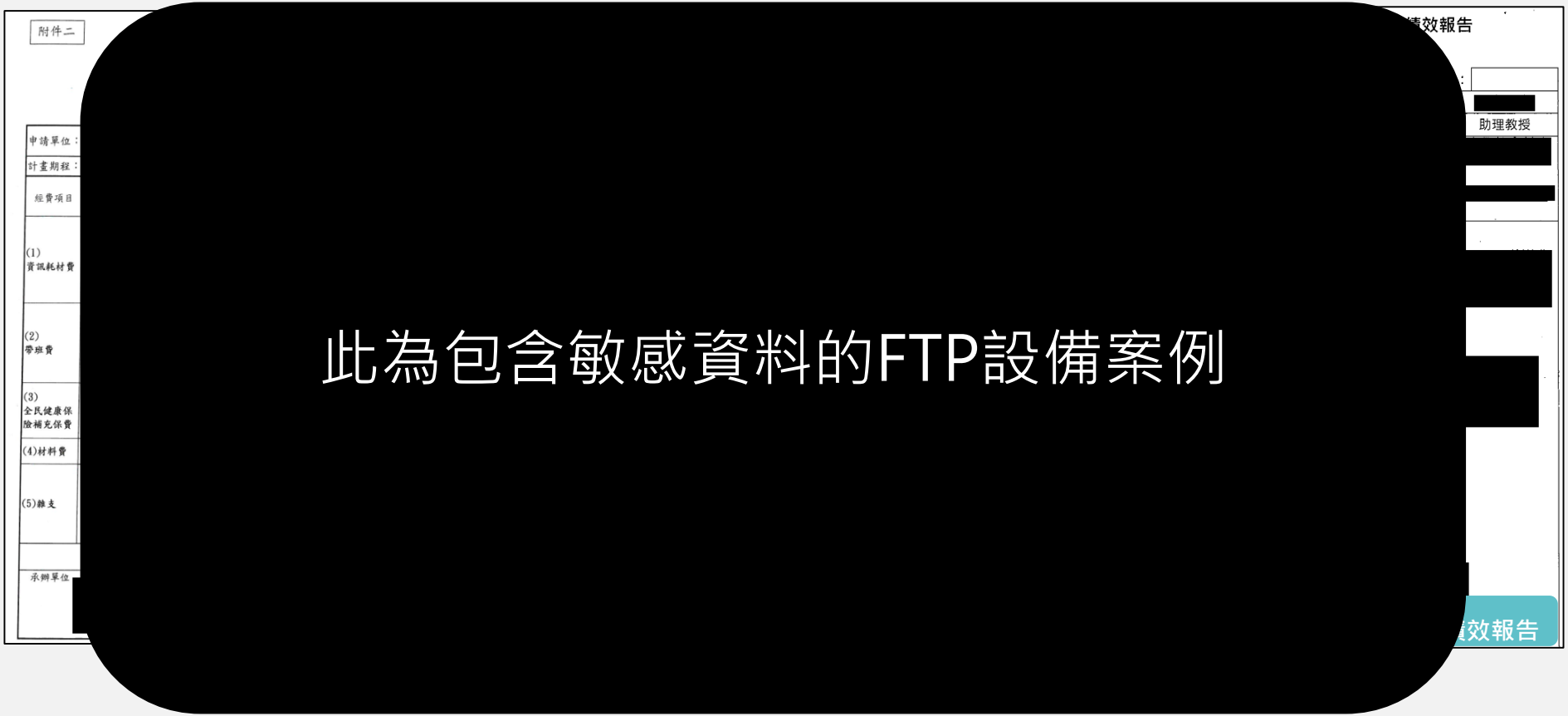
- 避免將設備的**管理介面**暴露於**公開網路**上。
- 應定期(或請廠商協助)檢視組態設定是否符合資安要求。
- 採購設備時應請廠商修補已知的漏洞。
- 定期執行設置檔備份與更新韌體。
- 機敏性資料應作適當的遮罩。
- 重要系統(尤其是包含機敏性資料)應做完弱點與源碼檢測後再上線。

FTP設備匿名登入(弱密碼)通報

FTP 登入檢測(包含個資的案例)

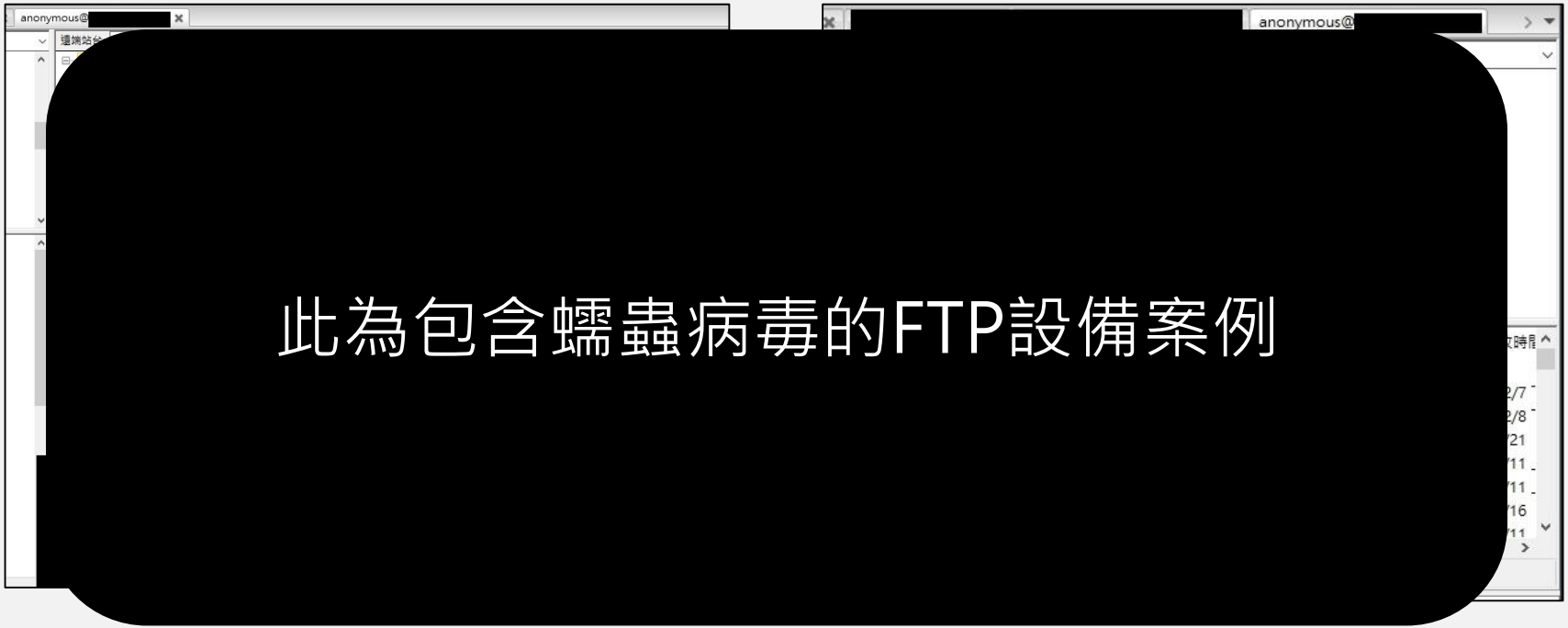


FTP 登入檢測(包含敏感資料的案例)



FTP 登入檢測(PhotoMiner蠕蟲病毒)

- 隨機對暴露在公開網路上使用FTP協定的IP，以內建的帳號密碼字典檔進行暴力破解攻擊，若使用弱密碼或匿名登入容易被此類型的蠕蟲病毒入侵。



參考網址：https://portal.cert.tanet.edu.tw/docs/pdf/20170929010955558577122890605 1.pdf

建議與結論

- 建議將設備放置於內部網路，若有外部網路存取需求，請限定連線IP(ACL)。
- 關閉預設帳號與匿名登入服務，並使用強度較高的密碼。
- 若有放置機敏性資料的需求，請進行加密或作適當的遮罩，並於使用完畢後移除以降低風險。
- 依據檔案的重要性與機密性建立權限控管機制。
- 定期檢視系統稽核紀錄降低資安風險。

TANet

謝謝聆聽

THANK YOU FOR LISTENING

臺灣大學計算機及資訊網路中心

報告人：陳思蘊

2023年 07月 05日

MINISTRY OF EDUCATION 教育部

國立臺灣大學 教學品質・學術卓越・人文關懷・愛國愛校