區網會議

IoT 物聯網設備風險現況與防範策略

2025/06/25

IoT設備介紹

物聯網的定義

- 物聯網(Internet of Things)以下簡稱 IoT，廣義的定義為「可透過各種連線方式連接網路的設備」皆可視為 IoT 裝置，例如:網路攝影機(監控系統)、印表機(事務印表機)、網路附加儲存設備(NAS)、無線網路(Wifi)分享器、數位電子看板、能源管理系統等等。
- IoT 的目的是為了「透過將真實的物體聯結上網，以達到控制分享、 分析及應用」。

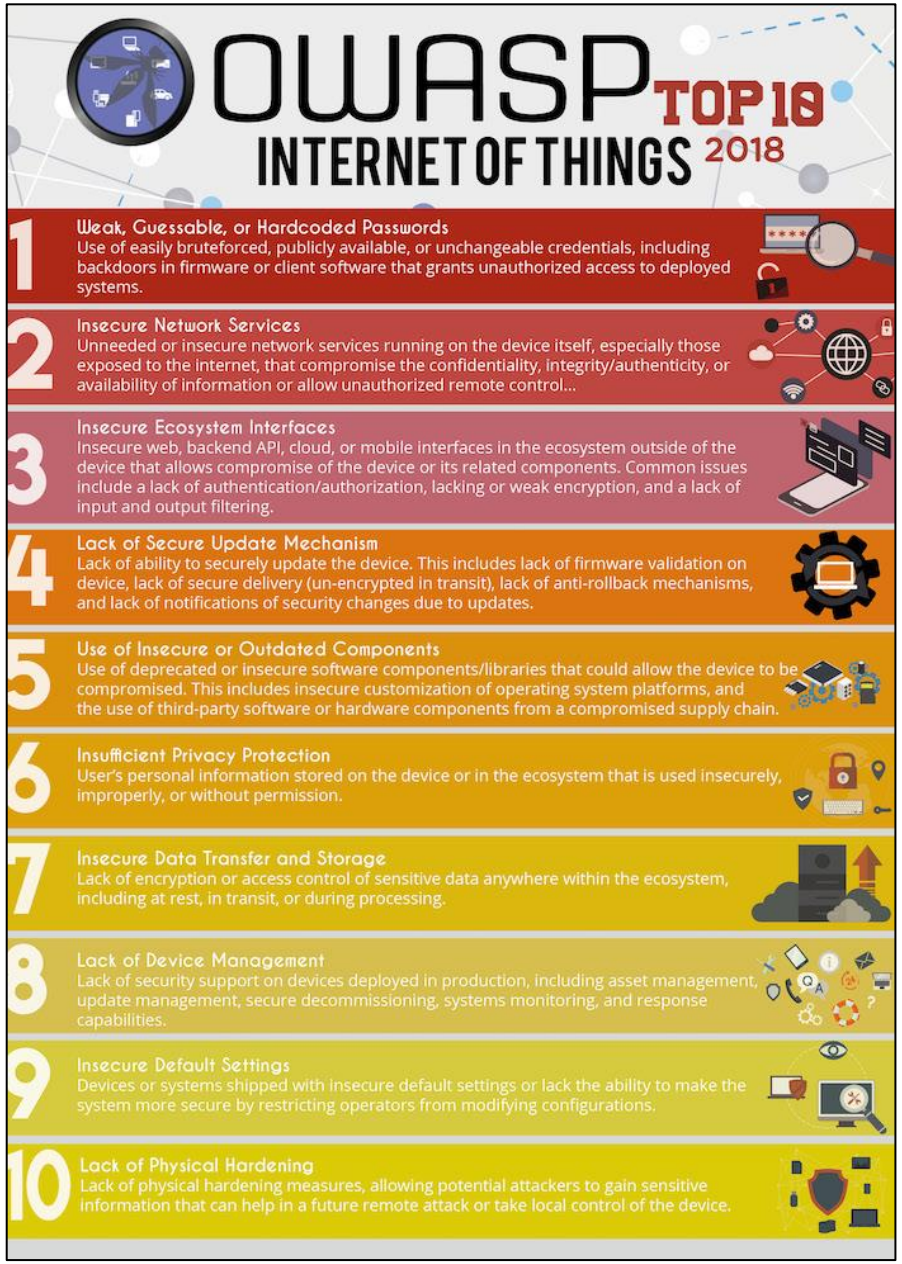
https://portal.cert.tanet.edu.tw/docs/pdf/2022110404114040719862739608309.pdf
http://www.business2community.com

IoT 設備特性

- 網路連接能力
  - 透過Wi-Fi、藍芽、或使用IP協定與其他裝置或伺服器溝通
- 資料感測與收集
  - 搭配各式各樣的感測器，持續或定時收集狀態資訊
- 自動化與遠端控制
  - 透過遠端或自動化執行服務
  - 透過APP、Web UI進行遠端控制
- 嵌入式系統設計
- 規模龐大

OWASP TOP 10
Internet of Things 2018

OWASP TOP 10 Internet of Things 2018



TOP 1：Weak, Guessable, or Hardcoded Passwords

- 說明：

  裝置使用容易被猜出、預設、公開或無法變更的密碼，例如 ：admin/admin。

  某些產品預設出廠使用固定帳密(或無帳密)，攻擊者利用 Shodan 即可找到使用IP並透過Google搜尋預設帳密即可登入。
- 建議防護措施：
  - 上線前強制修改帳號密碼
  - 禁用硬編碼(直接寫死在程式碼內)的帳密
  - 啟用登入鎖定與 MFA(多因子驗證)機制

TOP 2：Insecure Network Services

- 說明：

  設備開放不必要或不安全的網路服務（如: Telnet、未加密的 HTTP），導致資料洩漏或遠端控制風險。

  物聯網設備開啟 port 23（Telnet），成為殭屍網路一部分。
- 建議防護措施：
  - 關閉未使用的服務
  - 使用防火牆過濾
  - 僅允許使用加密協定（如 HTTPS、SSH）

TOP 3：Insecure Ecosystem Interfaces

- 說明：

  感測器(Sensor)、API、雲端、行動 App 等介面未妥善驗證用戶、缺乏加密或呈現過多且不必要的資訊。

  物聯網設備之API，無進行身分驗證即可查詢所有裝置狀態與資訊。
- 建議防護措施：
  - 強化身份驗證機制
  - 加密傳輸資料
  - 實作 API Rate Limiting

CVE漏洞簡介

CVE
Common Vulnerabilities and Exposures

- 由美國 MITRE (非營利機構)主導與維護
- 漏洞編號組成CVE+2025+12345
- Known Exploited Vulnerabilities Catalog
  - 已分配CVE編號
  - 漏洞已有被廣泛利用的跡象
  - 漏洞有明確的修補措施，或已提供更新

平台/工具	嚴重程度
NVD	• CVSS 評分 • 漏洞細節 • 修補建議
MITRE CVE	漏洞基本資訊
Exploit-DB GitHub	漏洞PoC
Nessus OpenVas	漏洞檢測工具

CVSS
Common Vulnerability Scoring System

- CVSS v3.x分數組成：
- **基本評分(Base Score)**
  - **攻擊向量（Attack Vector, AV）**
  - **攻擊複雜度（Attack Complexity, AC）**
  - **所需權限（Privileges Required, PR）**
  - **使用者互動（User Interaction, UI）**
  - **影響程度（機密性C、完整性I、可用性A）**
- 時間評分(Temporal Score)
  - 漏洞修補狀態、攻擊代碼成熟度等
- 環境評分(Environmental Score)
  - 對特定組織環境的影響調整（是否部署了緩解措施）

分數範圍	嚴重程度
0.0	無風險
0.1-3.9	低(Low)
4.0-6.9	中(Medium)
7.0-8.9	高(Hight)
9.0-10.0	嚴重(Critical)

https://nvd.nist.gov/
https://cve.mitre.org/

CVE-2024-4577 x CVSS v3.x

CVE-2024-4577 Detail

Description

In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in command line given to Win32 API functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to PHP binary being run, and thus reveal the source code of scripts, run arbitrary PHP code on the server, etc.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: PHP Group **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

References to Advisories, Solutions, and Too

By selecting these links, you will be leaving NIST webspace. We have provided these have information that would be of interest to you. No inferences should be drawn on acc from this page. There may be other web sites that are more appropriate for your purpose. NIS xpressed, or concur with the facts presented on these sites. Further, NIST does not endorse an ned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink
http://www.openwall.com/lists/oss-security/2024/06/07/1

QUICK INFO

CVE Dictionary Entry:
CVE-2024-4577
NVD Published Date:
06/09/2024
NVD Last Modified:
03/28/2025
Source:
PHP Group

https://nvd.nist.gov/vuln/detail/cve-2024-4577

IoT設備相關資安新聞

居家監視器、掃地機器人遭入侵

https://www.youtube.com/watch?v=-3a5ruQBty0

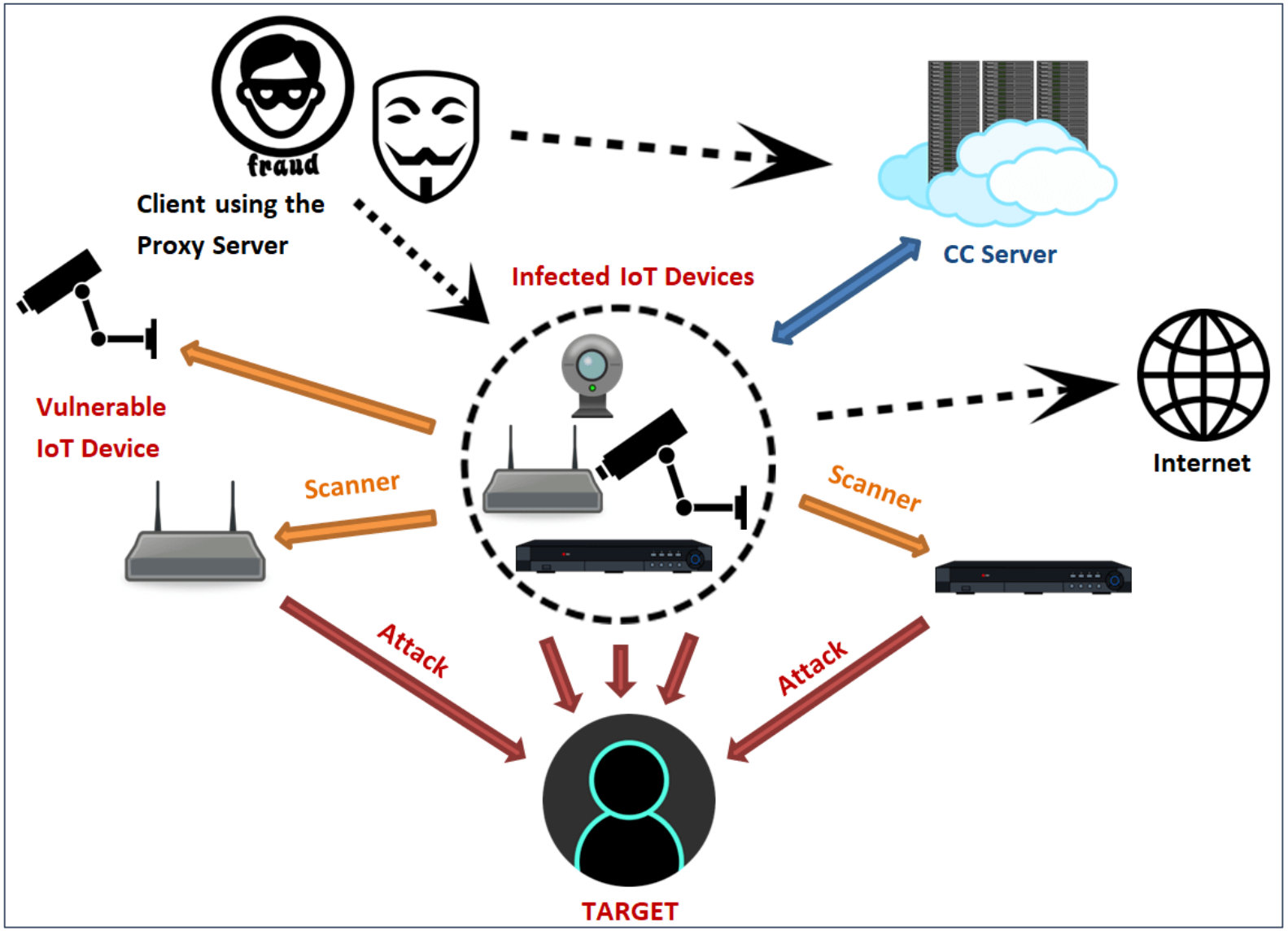
IoT設備 x Mirai殭屍網路

超過 50 萬個IoT設備
組成殭屍網路Mirai

DDoS攻擊
Minecraft伺服器

https://www.bbc.com/news/technology-38678466

Mirai變種版本感染方式



https://zh.wikipedia.org/wiki/Mirai_(%E6%81%B6%E6%84%8F%E8%BD%AF%E4%BB%B6)
https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers

檢測方法 與 案例分享

IoT搜尋引擎

- **Shodan(https://www.shodan.io/)**
- Censys(https://censys.com/)
- Fofa(https://fofa.info/)
- ZoomEye(https://www.zoomeye.ai/)

IoT搜尋引擎
Shodan學術帳號

- 申請一般帳號

學術升級

Shodan 為使用學術電子郵件地址（例如以 結尾的地址等）註冊的用戶提供免費的會員升級服務，學術會員資格包括以下內容： `.edu` `.ac.uk`

- 能夠監控最多 16 個 IP
- 每月 100 個查詢積分
- 每月 100 次掃描積分
- 訪問Shodan 地圖和Shodan 圖像
- `vuln` 可以在網站上使用過濾器

https://help.shodan.io/the-basics/academic-upgrade

IoT搜尋引擎
Shodan常用查詢參數 x 常用連接埠

參數	說明	範例
net	IP位置或網段	net:123.23.1.0/24
port	連接埠	port:21
product	作業系統/軟體名稱	product:windows
country	國家	country:tw
city	城市	city:"Taipei"
org	組織或公司	org:google
hostname	主機名稱	hostname:www.edu.tw
org	組織或公司	org:google
http.title	網站標題	http.title:"hacked by"
vuln	漏洞編號	vuln:CVE-2014-0160

連接埠	說明
21	FTP
80 443 8080 8443 5000 5001	HTTP/HTTPS 管理介面/資訊頁
554	RTSP
22	SSH
23	TELNET
515	LPD
631	IPP
9100	PDL
161	SNMP
1900	UPnP

https://www.shodan.io/search/examples

SNMP(161)

- 監控與管理網路設備(如:路由器、交換器、伺服器、印表機等)的協定，但若未妥善設定或保護，會帶來許多資安風險。
- 使用預設社群字串(community string)
- SNMPv1/v2 傳輸內容未加密
- 未限制 SNMP 存取來源

- SnmpWalk

UPnP(1900)

- 通用隨插即用(Universal Plug and Play)
- 使家庭網路(資料共享、通訊和娛樂)和公司網路中的各種裝置能夠相互無縫連接，並簡化相關網路的實現。
- 不安全的自動埠轉發(Port Forwarding)
- UPnP 設定可從外部存取(External Exposure)
- 各類型的漏洞
- 無身份驗證與存取控制

- nmap

網路攝影機(監控系統)

IoT搜尋引擎
Shodan-網路攝影機(IP Cam)

協定/服務	說明	Shodan 查詢語法
RTSP	網路協定，用來控制多媒體串流伺服器上的媒體播放。	RTSP port:554
UPnP	通用隨插即用協定	port:1900
SNMP	監控與管理設備之協定	port:161 "public"
Web 管理介面	預設啟用 Web UI (通常為 port 80、443、8080)	http.title:printer
		port:80、port:443、port:8080
根據廠牌或型號搜尋	廠牌名稱	TP-Link、D-Link

https://www.shodan.io/dashboard

攝影機/影像監控設備(IP Cam)
預設帳密

1 2 3 4 5 6 7 8 9 »

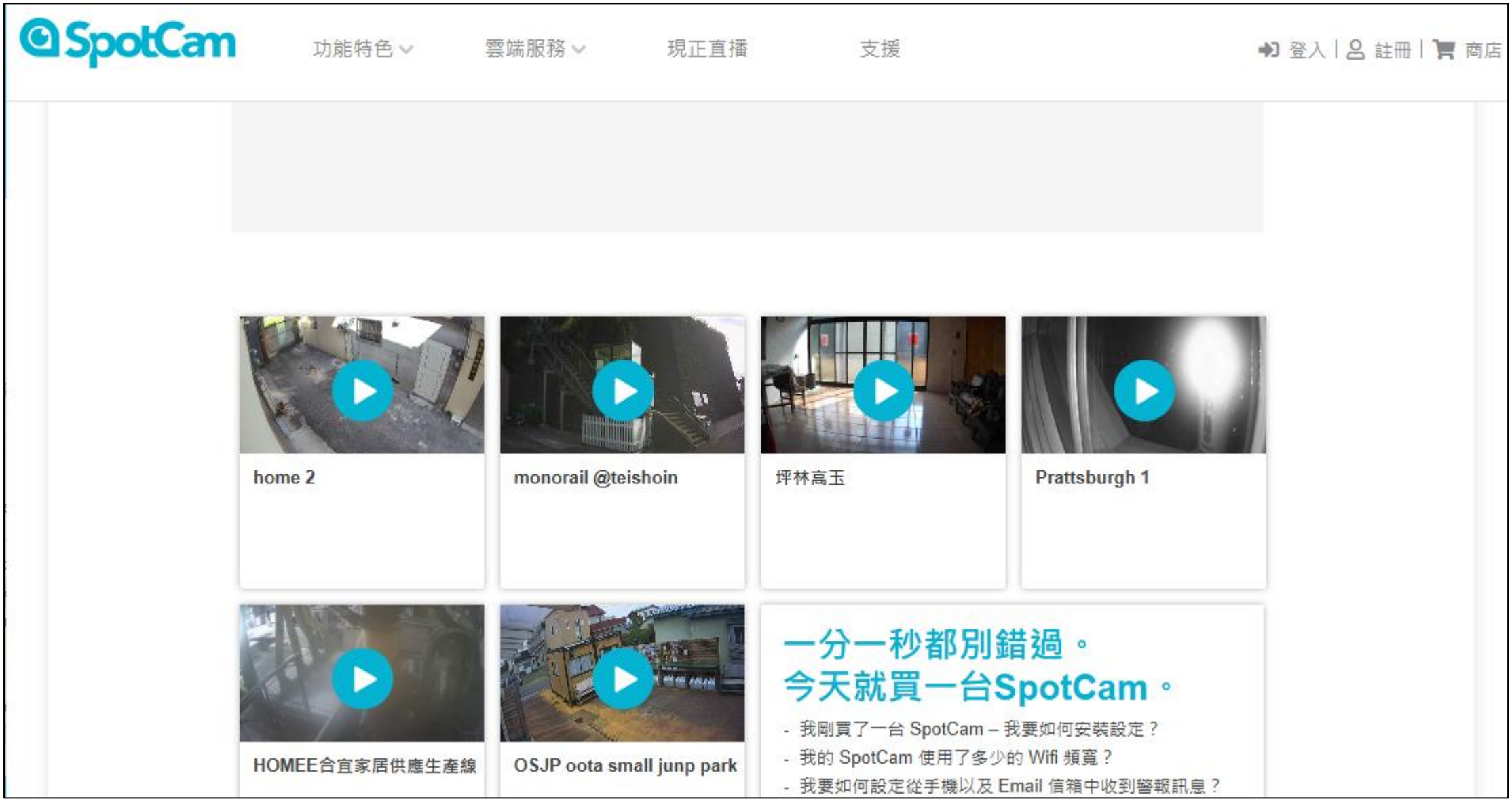
Live camera in Taipei, Taiwan, Province Of

Live camera in Chiayi, Taiwan, Province Of

Live camera in Taipei, Taiwan, Province Of

http://www.insecam.org/en/bycountry/TW/

攝影機/影像監控設備(IP Cam)
直播串流



https://www.myspotcam.com/tc/onair?category=Destinations

IP Cam
資安威脅

- Web UI 或遠端存取可透過預設帳密或無帳密登入
- 未修補的韌體漏洞
- 影像資料外洩
- 殭屍網路(Botnet)

印表機(事務印表機)

IoT搜尋引擎
Shodan-印表機(Printer)

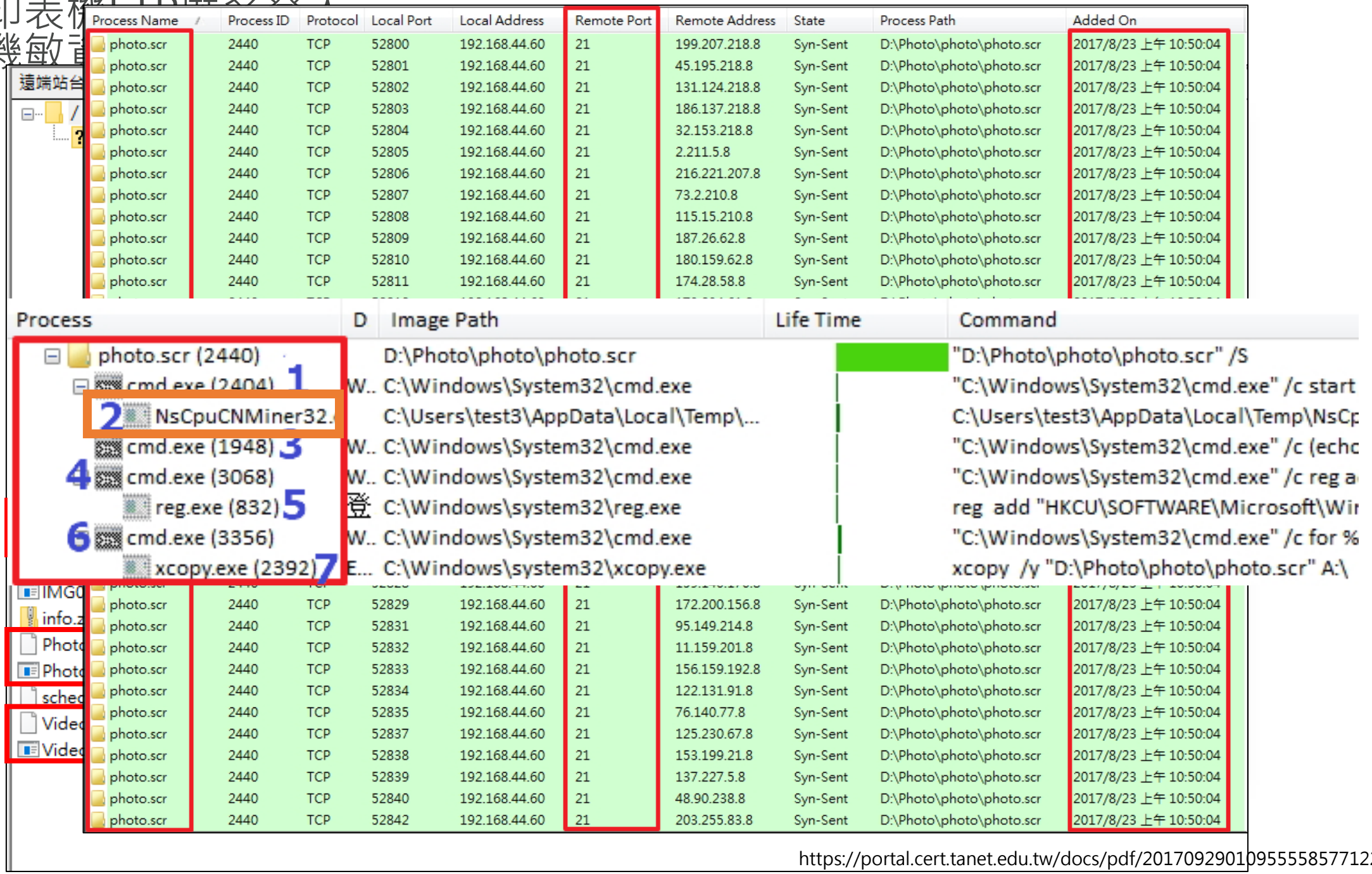
協定/服務	說明	Shodan 查詢語法
JetDirect	HP 等印表機使用的印表通訊協定	port:9100
IPP (Internet Printing Protocol)	現行印表機常用，網際網路列印協定	port:631 ipp
LPD (Line Printer Daemon)	舊款印表機常用協定	port:515
UPnP	通用隨插即用協定	port:1900
SNMP	用於印表機狀態監控，很多印表機預設開啟	port:161 "public"
Web 管理介面	印表機預設啟用 Web UI （通常為 port 80、443、8080）	http.title:printer
		port:80、port:443、port:8080
根據廠牌或型號搜尋	如：Kyocera、HP、Canon、Epson	Kyocera、HP、Canon、Epson

https://www.shodan.io/dashboard

Printer
資安威脅

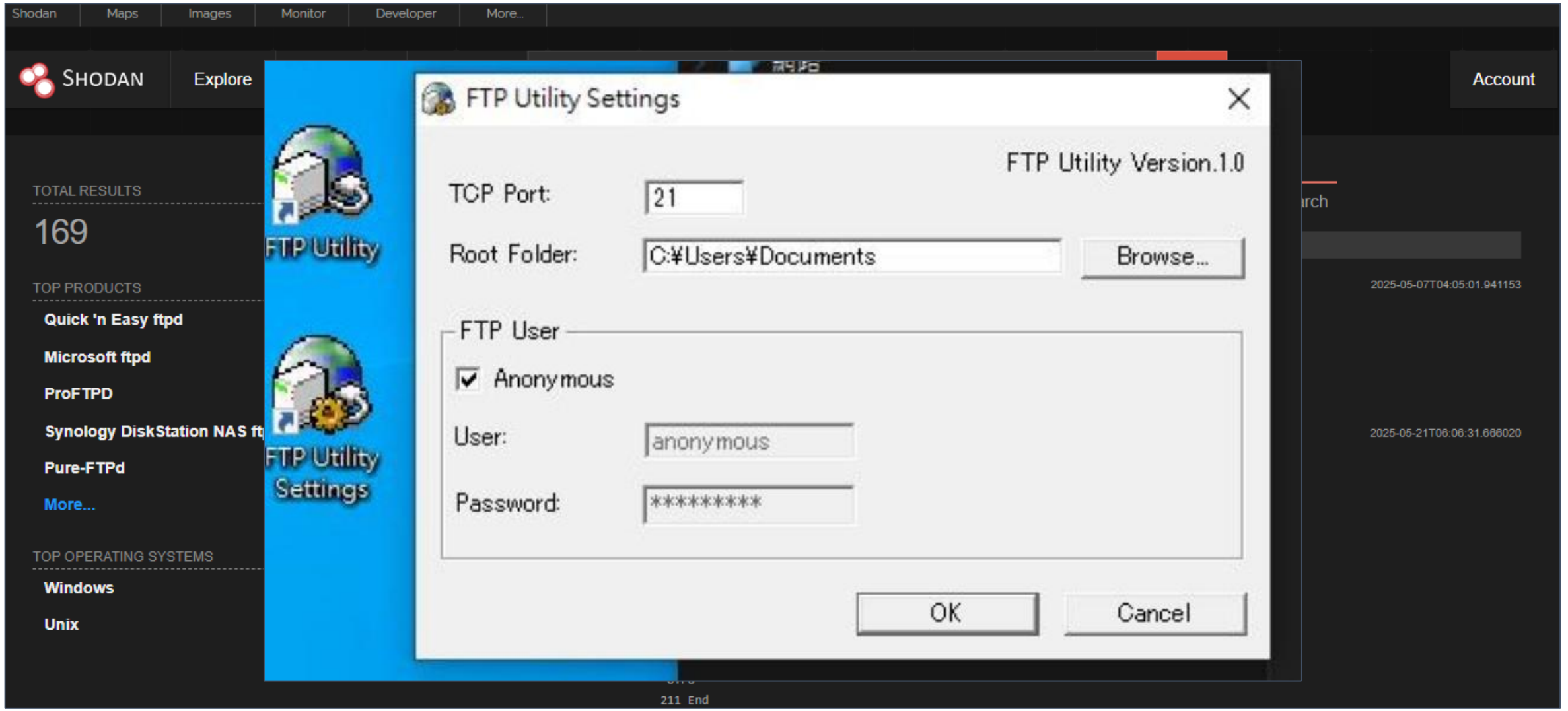
- Web UI 或遠端存取可透過預設帳密或無帳密登入
- 未加密的網路服務
  - 自動列印(9100 JetDirect)
  - 取得印表機狀態與機密資訊(161 SNMP)
- 未修補的韌體漏洞
- 印表機掃描檔案未加密或限制存取
- 殭屍網路(Botnet)

印表機FTP歷名登入
機敏資



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

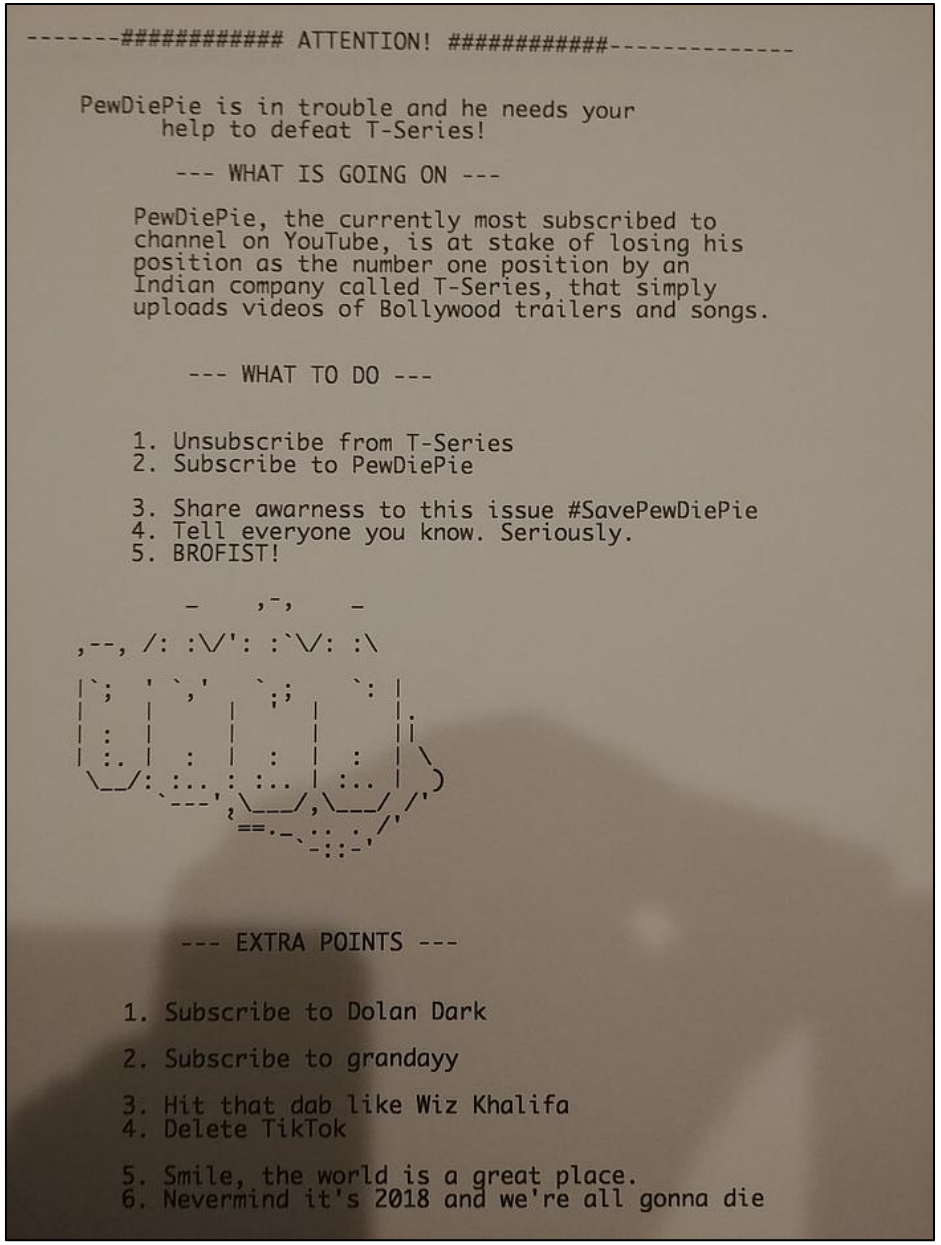
IoT搜尋引擎
Shodan-FTP檔案傳輸協定



port:21 net:140.x.x.0/16

https://www.shodan.io/
https://www.cc.ntu.edu.tw/chinese/epaper/home/20210620_005705.html

印表機駭客



https://shadowmaster98.medium.com/printer-hacking-101-b4faf4f3fcdc
https://www.ithome.com.tw/news/127458

網路附加儲存設備
(Network Attached Storage, NAS)

IoT搜尋引擎
Shodan-NAS(Network Attached Storage)

協定/服務	說明	Shodan 搜尋語法
Web 管理介面	NAS Web UI (HTTP/HTTPS)	http.title:nas 或 http.title:"Web File Manager"
FTP	NAS 啟用FTP 通訊協定	port:21 ftp nas
SMB	Windows 網路共享 如：Synology/QNAP	port:445
AFP	Apple 文件傳輸協定 (舊型 NAS)	port:548
SSH	管理介面或遠端維護	port:22 "nas"
UPnP	NAS通用隨插即用協定	port:1900
Telnet	舊款 NAS 未保護的 Telnet通訊協定	port:23 "nas"
根據廠牌與型號搜尋	Synology、QNAP、ASUSTOR、Netgear	http.title: “Synology DiskStation” 、 product:"Synology"

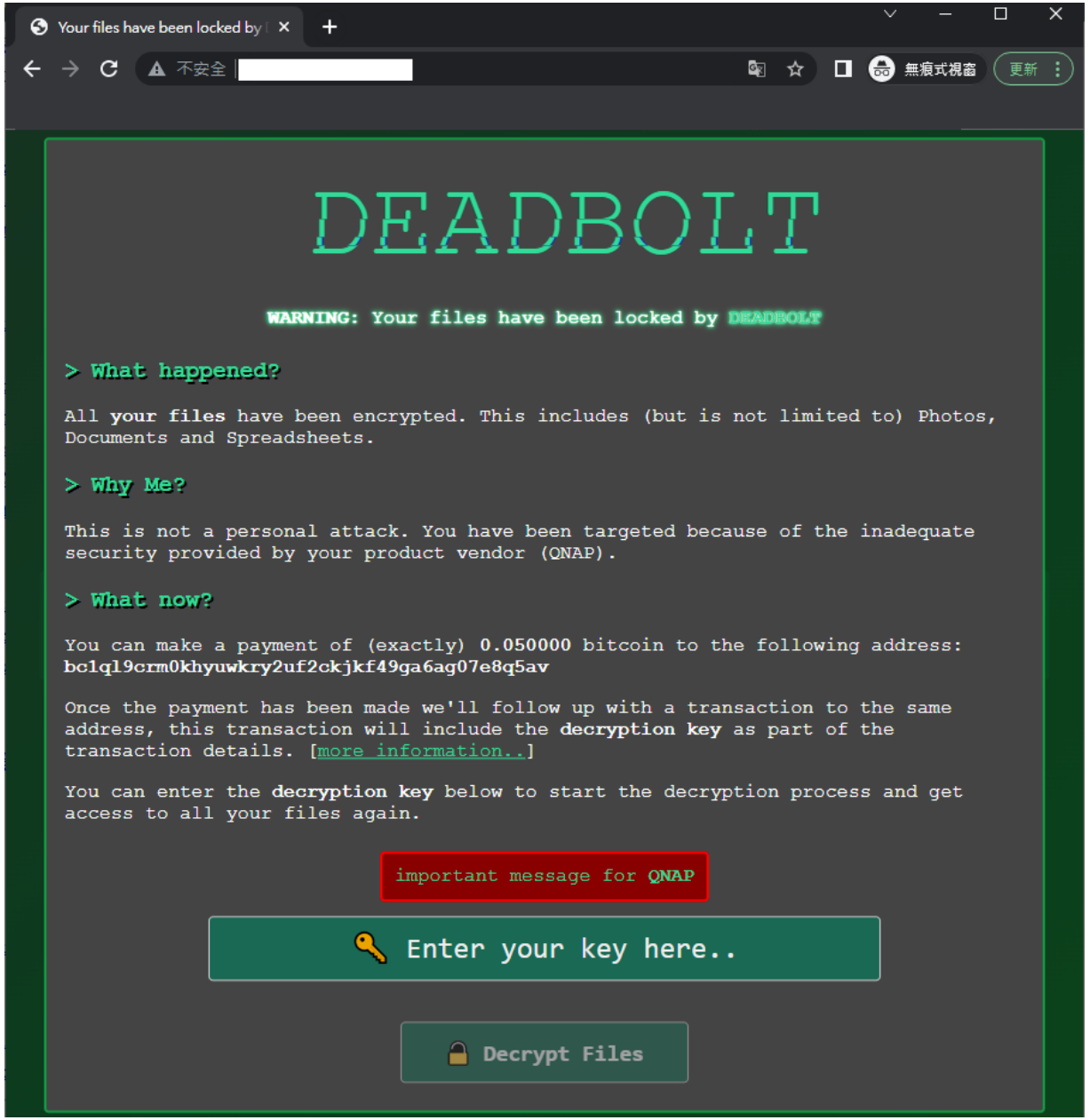
https://www.shodan.io/dashboard

NAS(Network Attached Storage)
資安威脅

- Web UI 未加密或無密碼保護
- FTP/SMB 無登入驗證
- Telnet/SSH 開啟且使用預設帳密（如 admin/admin）
- 裝置洩漏版本資訊與品牌，容易被針對攻擊

  （如: QNAP 遭勒索病毒攻擊）
- 殭屍網路(Botnet)

DEADBOLT
勒索軟體



```
Nmap scan report for us[redacted].edu.tw (140.[redacted])
Host is up (0.0025s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 192.168.147.231 is not the same as 140.[redacted]

Nmap scan report for ftp.ntu.edu.tw (140.[redacted])
Host is up (0.0030s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 192.168.110.102 is not the same as 140.[redacted]

Nmap scan report for 140.[redacted]
Host is up (0.0030s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxrwxrwx   1 SYSTEM   SYSTEM       5826390 Sep 22  2016 1050922\xA8t\xB0\xC8\xB7|\xC4\xB3\xC4\xB3\xB5{.pdf [NSE: writeable]
| -rwxrwxrwx   1 alicelin alicelin    13536667 May 12 11:47 3.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1913258 Oct 18  2013 SCAN20131018163139.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        236733 Nov 13  2013 SCAN20131113101833.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        246973 Nov 13  2013 SCAN20131113101900.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        236733 Nov 13  2013 SCAN20131113101920.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        462686 Nov 13  2013 SCAN20131113101954.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        730272 Nov 13  2013 SCAN20131113102043.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        329566 Nov 13  2013 SCAN20131113102137.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        175293 Nov 13  2013 SCAN20131113102632.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1192419 Nov 13  2013 SCAN20131113102658.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1018339 Nov 13  2013 SCAN20131113102814.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        935745 Nov 15  2013 SCAN20131115181414.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1470245 Nov 19  2013 SCAN20131119115314.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        175293 Dec 20  2013 SCAN20131220151442.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        267454 Dec 30  2013 SCAN20131230165836.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        226494 Dec 30  2013 SCAN20131230165902.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        267455 Dec 30  2013 SCAN20131230175645.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        134333 May 02  2014 SCAN20140502120926.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        720032 May 02  2014 SCAN20140502123746.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1470245 May 16  2014 SCAN20140516141624.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        360286 May 16  2014 SCAN20140516154547.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        216253 May 16  2014 SCAN20140516160020.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        216253 May 16  2014 SCAN20140516160047.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        216253 May 16  2014 SCAN20140516160102.pdf [NSE: writeable]
```

nmap.org/

無線網路分享器
(Wireless AP)

IoT搜尋引擎
Shodan-Wireless AP

協定/服務	說明	Shodan 搜尋語法
Web 管理介面	Wireless(AP) Web UI (HTTP/HTTPS)	http.title:"Access Point “ port:8443 port:80
SSH	遠端存取	port:22
Telnet	Telnet通訊協定	port:23
SNMP	查詢 SSID、MAC、機型	port:161 snmp
UPnP	通用隨插即用	Port:1900
根據廠牌與型號搜尋	MikroTik、ASUS、D-LINK	RouterOS、ASUS、title:"D-LINK SYSTEMS"

https://www.shodan.io/dashboard

Wireless AP
資安威脅

- Web UI 未加密或無密碼保護
- Telnet/SSH 開啟且使用預設帳密（如 admin/admin）
- 裝置洩漏版本資訊與品牌，容易被針對攻擊
- Man-in-the-middle attack， MITM 中間人攻擊
- 殭屍網路(Botnet)

Wi-Fi溢波(無線AP)

警政報馬仔

發布日期：112-

刑事局偵破影

刑事局偵破國內知
享器的連線安全
國內最大線上影
志埕表示，本案
商家Wi-Fi無線網
戶資料及影視資
刑事局呼籲商家
路的不法工具。

識，提升Wi-Fi分

大隊副大隊長陳
工程師，入侵某
間，刪除公司用

入侵他人電腦網

刑事警察局

臺北市政府警察局 刑事警察大隊
Criminal Investigation Division, Taipei City Police Department

如何提升Wi-Fi無線網路安全，避免自家網路成為駭客犯罪跳板？

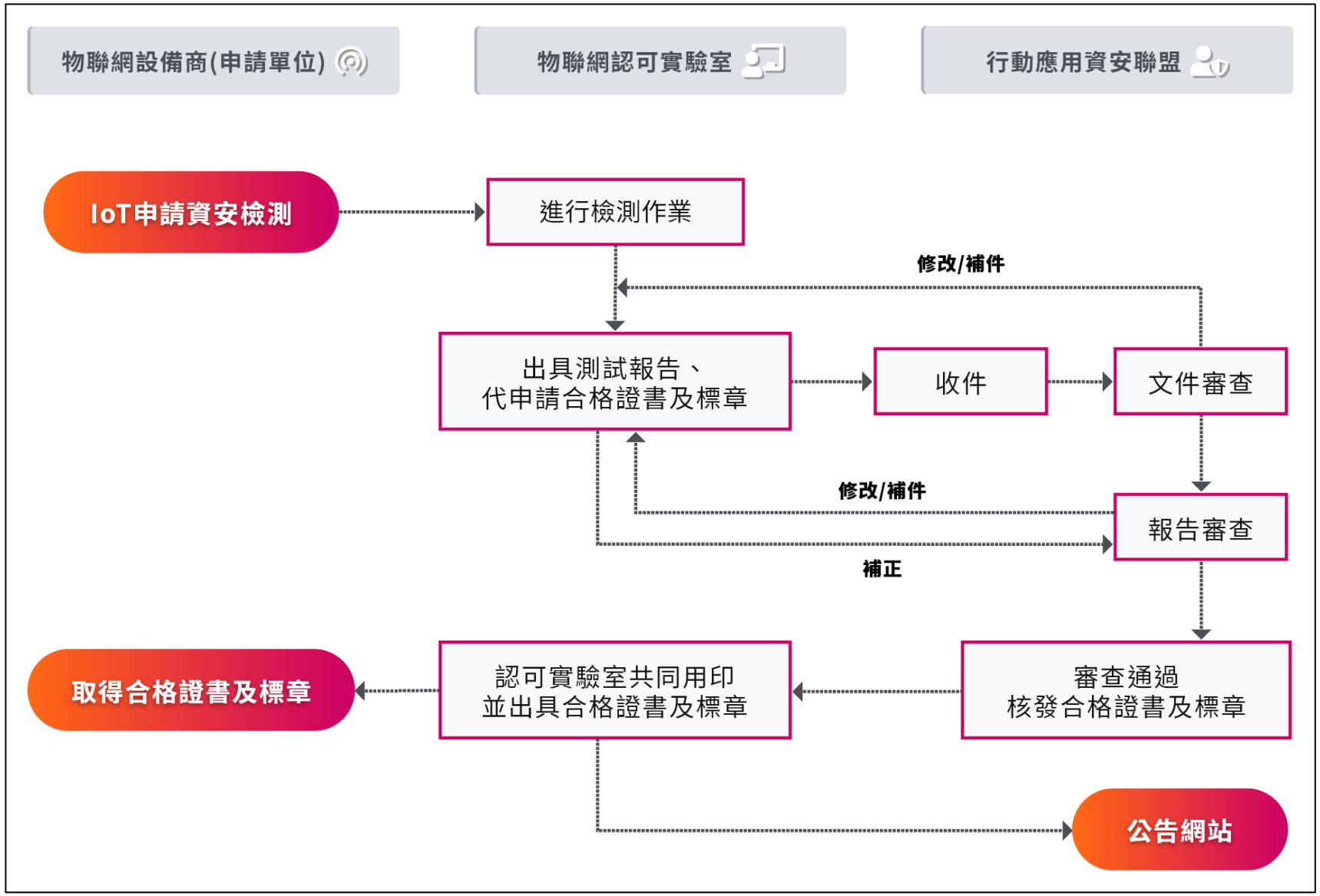
Wi-Fi僅供消費顧客使用，
避免將連線密碼公開於網路

儘可能定期變更連線密碼，
非營業時間關閉Wi-Fi連線

https://www.pbs.npa.gov.tw/

防範攻擊策略

IoT 設備安全標章
行動應用資安聯盟



https://www.mas.org.tw/iot/applicationProcedures

IoT 設備安全標章
台灣資通產業標準協會

表 1 安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
實體安全	5.1.1. 實體埠之安全管控	-	5.1.1.2	-
	5.1.2. 實體異常行為警示	-	-	-
	5.1.3. 實體防護	-	5.1.3.2	-
	5.1.4. 安全啟動	-	-	-
系統安全	5.2.1. 作業系統與網路服務安全	-	-	-
	5.2.2. 網路服務連接埠安全	-	-	-
	5.2.3. 更新安全	-	-	-
	5.2.4. 敏感性資料儲存安全	-	-	-
	5.2.5. 網頁管理介面安全	-	-	-
	5.2.6. 操控程式之應用程式安全	-	-	-
	5.2.7. 日誌檔與警示	-	-	-
通訊安全	5.3.1. 敏感性資料傳輸安全	-	-	-
	5.3.2. 通訊介面的安全設置	-	-	5.3.2.2
	5.3.3. 通訊協定安全	-	-	-
身分鑑別與授權機制安全	5.4.1. 鑑別機制安全	-	-	-
	5.4.2. 通行碼鑑別機制	-	-	-
	5.4.3. 權限控管	-	-	-
隱私保護	5.5.1. 隱私資料的存取保護	-	5.5.1.2	-
	5.5.2. 隱私資料的傳輸保護	-	-	-

IoT設備攻擊防範建議

- 定時更新軟(韌體)版本
- 加強登入密碼的強度，或啟用多重要素驗證(MFA)驗證機制
- 使用虛擬IP，關閉非必要的連接埠
- 變更或停用不安全的預設設定
- 限制IP連線存取，以及權限控管
- 建議採購包含完整安全檢測之產品

感謝聆聽!