內網印表機狂噴攻擊代碼致資源耗盡：事件調查與防護建議

2025/05/12

黃O弘

【一、事件背景】

- 2025/04/24 清晨發現多台內網印表機遭入侵行為觸發，自動巨量列印出目錄遍歷、帳號破解等攻擊指令，初判內部設備遭惡意控制。
- 目前已知涉及印表機（均屬 172.20.XX.XX 區段）：
  - 電算中心秘書室印表機
  - 電算中心二樓大印表機
  - 電算中心一樓大印表機
  - 教務處等其他單位數台印表機

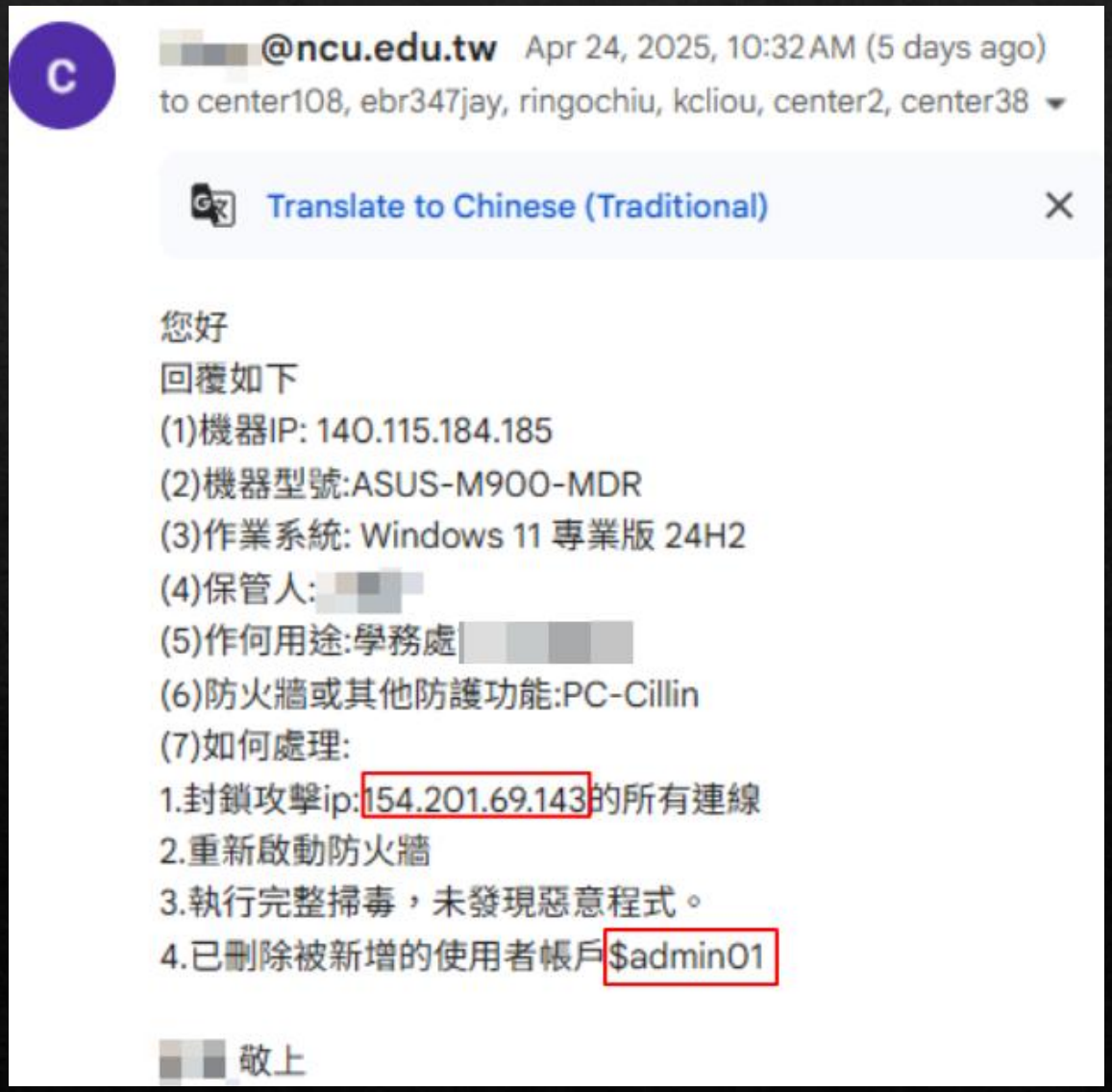
【二、資安通報】

教育機構資安通報平台

事件類型:入侵事件警訊

原發布編號	NTUSOC-102-202504-ntuasoc-20250423-164902	原發布時間	2025-04-24 08:15:13
事件類型	惡意程式	原發現時間	2025-04-24 00:00:23
事件主旨	教育部資安通告-國立中央大學[140.115.184.185]主機進行惡意程式連線(MALWARE-CNC Win.Trojan.VShell variant outbound connection attempt)		
事件描述	原始紀錄:MALWARE-CNC Win.Trojan.VShell variant outbound connection attempt,入侵偵測防禦系統偵測到來源IP(140.115.184.185)，包含疑似惡意程式連線行為特徵之封包，對目標IP(154.201.69.143)進行連線，原始事件觸發時間：2025-04-23 16:49:04。此事件來源 PORT(53918)，目標 PORT(8080)。		
手法研判			
建議措施	請檢視來源IP該連線行為是否已得到合法授權。 若來源IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查： a.請查看來源IP有無異常動作(如：新增帳號、開啟不明Port、執行不明程式)。 b.確認防毒軟體的病毒碼已更新為最新版本，並進入系統安全模式下行進行全系統掃描作業、系統是否已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。 若來源IP為DNS server、NAT主機或IP分享器等設備IP時，表示有內部主機透過這些設備向外連線時而觸發偵測規則， 則需先請設備管理者透過事件單所附之資訊(目的地IP、時間、來源port)，來協助查找內部觸發偵測規則之主機，再依前述建議處理措施進行作業。		

【三、學務處回報】



C

[redacted]@ncu.edu.tw Apr 24, 2025, 10:32 AM (5 days ago)

to center108, ebr347jay, ringochiu, kcliou, center2, center38

Translate to Chinese (Traditional)

您好
回覆如下
(1)機器IP: 140.115.184.185
(2)機器型號:ASUS-M900-MDR
(3)作業系統: Windows 11 專業版 24H2
(4)保管人:[redacted]
(5)作何用途:學務處[redacted]
(6)防火牆或其他防護功能:PC-Cillin
(7)如何處理:
1.封鎖攻擊ip:154.201.69.143的所有連線
2.重新啟動防火牆
3.執行完整掃毒，未發現惡意程式。
4.已刪除被新增的使用者帳戶$admin01

[redacted] 敬上

【四、安全性紀錄】

1. 電算中心秘書室印表機的安全性紀錄進行溯源分析
2. 發現來源 IP 140.115.184.185 於 4/24 凌晨異常大量連線並列印
3. 列印內容為典型的滲透測試指令與目錄遍歷攻擊樣態
4. 巧合發現 140.115.184.185 為已遭入侵之學務處主機

【五、攻擊樣本初步分析-1】

```
GET /systemController/showOrDownByurl.do?down=&dbPath=../../../../../../etc/pa
Host: 172.20.11.238:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Accept-Encoding: gzip
```

分析：

➡️ GET 請求：攻擊者發送一個 HTTP 讀取指令，目標呼叫 /systemController/showorDownByurl.do，並透過參數 dbPath=../../../../../../etc/passws 執行目錄跳脫（../ 用於返回上層目錄），

企圖讀取 /etc/passwd。

➡️ Host：目標伺服器為 172.20.11.238，使用 9100 埠（原本為 DIPRINT 列印用途，於此次被濫用作為攻擊指令傳輸通道）。

✅ 小結

攻擊者偽裝成一般正常請求，實際結合 GET 指令與目錄跳脫技巧，試圖直接存取系統敏感檔案 /etc/passwd，屬於典型的目錄遍歷攻擊（Directory Traversal Attack）。

【五、攻擊樣本初步分析-2】

```
GET /Audio/1/hls/..%5C..%5C..%5C..%5C..%5C..%5CWindows%5Cwin.ini/stream.mp3/ H
Host: 172.20.11.238:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Accept-Encoding: gzip
```

分析：

➡️ **GET 請求：攻擊者向 /Audio/1/hls/..%5C..%5C..%5C..%5Cwindows%5Cwin.ini/stream.mp3 發送讀取指令，企圖透過多層目錄跳脫（%5C 為 URL 編碼的反斜線 \，用於模擬 Windows 路徑結構），存取 Windows 系統設定檔 C:\Windows\win.ini。**

✅ 小結

攻擊者利用目錄跳脫技術，嘗試讀取 Windows 系統內部設定檔 win.ini，驗證目錄存取控制是否鬆散，屬於目錄遍歷攻擊（Directory Traversal Attack）**的常見探測手法。**

【五、攻擊樣本初步分析-3】

```
POST /login.php HTTP/1.1
Host: 172.20.11.238:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
Content-Length: 50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

username=admin&password=admin?show+webmaster+user
```

分析：

➡️ **POST** 請求：攻擊者向 **/login.php** 發送登入表單，**帳號（username）和密碼（password）都設定為 admin，為典型的預設弱密碼嘗試**。

➡️ 傳送內容：後方夾帶 **?show+webmaster+user**，推測嘗試在登入後進行額外操作或注入指令（例如列出系統管理者帳號）。

✅ 小結：攻擊者以 **admin:admin** 組合嘗試暴力登入（**Brute Force**），並可能試圖利用弱驗證點進行指令注入。

屬於典型的**弱密碼暴力破解攻擊加橫向探索嘗試**。

【五、攻擊樣本初步分析-4】

```
POST /inter/ajax.php?cmd=get_user_login_cmd HTTP/1.1
Host: 172.20.11.117:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
Content-Length: 85
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

{"get_user_login_cmd":{"name":"admin","password":"21232f297a57a5a743894a0e4a80
```

🔍 分析：

➔ **POST 請求：攻擊者對 /inter/ajax.php 發送登入請求，傳送帳號（name）與密碼（password）。**

➔ **傳送內容：admin:21232f297a57a5a743894a0e4a801fc3（這是一組MD5雜湊值，對應明文密碼是 admin）**

➔ **目的推測：攻擊者嘗試使用 admin/admin 預設帳密登入，屬於典型弱密碼暴力測試行為。**

✅ 小結：

攻擊者試圖透過 admin/admin 這組弱密碼進行登入測試，顯示攻擊以弱點探測及暴力破解初步掃描為主，屬常見入侵前偵查行為。

【五、攻擊樣本初步分析-5】

```
POST /user.php HTTP/1.1
Host: 172.20.11.118:9100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTM
Content-Length: 39
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Referer: 45ea207d7a2b68c49582d2d22adf953aads|a:2:{s:3:"num";s:193:"*/SELECT 1,
Accept-Encoding: gzip

action=login&pp123=printf(43801*42758);
```

分析：

➔ **POST 請求：針對 /user.php 送出異常參數 pp123，試圖執行 printf(43801*42758);。**

➔ **攻擊方式：利用表單傳入惡意參數，試圖觸發遠端代碼執行漏洞（RCE）或指令注入。**

➔ **目的推測：如果伺服器端對輸入內容未做嚴格驗證，並且直接以 eval()、assert() 等方式執行參數，**

那麼即使單純的乘法運算也能被執行，進而證明伺服器正在解析並執行攻擊者傳入的內容，後續即可插入任意惡意指令。

✅ **小結：攻擊者明顯試圖以惡意參數注入觸發伺服器端執行非法運算，**

屬遠端程式碼執行（RCE）預備行為，危害等級高。

【六、資安執行小組及 SNMG 通報】

center108 <center108@ncu.edu.tw> Fri, Apr 25, 3:12 PM (4 days ago)

to

各位資安執行與 SNMG 小組成員您好：

昨日清晨，本校部分單位發生**印表機異常大量列印惡意內容**的狀況。

🧨 **攻擊情境如下：**

攻擊者疑似**入侵校內某台電腦後進行橫向移動**，並透過**內部網路大量發送列印命令**至單位印表機，使用協定為 **TCP Port 9100（DIPRINT / RAW 模式）**，導致印表機在數分鐘內**自動噴出上百張惡意 payload 內容**。

📌 **為避免再次發生，請各單位儘速採取以下資安防護措施：**

1️⃣ **限制來源 IP（最重要）**

- **請啟用印表機的防火牆或存取控制清單（ACL），僅允許貴單位所屬內部網段（例如資管系，140.115.80.X、140.115.82.X）連線與列印，並封鎖其他來源**

2️⃣ **停用 DIPRINT / RAW 模式（Port 9100）**

- 本次攻擊即透過 DIPRINT（TCP 9100）進行大量列印指令注入，**建議一律關閉此通訊埠**
- 請改用下列較安全之列印協定：
  - ✅ **LPR**（Port 515）
  - ✅ **IPP**（Port 631）
- 停用後，請使用者同步調整印表機設定，將通訊協定由 **RAW 改為 LPR**，並將 Queue Name 設為 `print`（小寫）；若單位導入 IPP，亦請協助切換使用。

3️⃣ **停用「訪客列印」或「未驗證列印」等開放式功能**

4️⃣ **更新印表機韌體**

5️⃣ **若尚未遷入 172.20.X.X 區段，請儘速完成遷移**

- 為強化印表機管理與存取控管，請各單位儘快將印表機**遷入校內統一規劃之 172.20.X.X 區段**
- ⚠️ 本次事件雖以**內網設備為主要攻擊目標**，但若印表機同時暴露於對外 IP 或開放存取，將面臨更嚴重資安風險

6️⃣ **強化印表機管理介面密碼與存取保護**

- 請確認印表機 Web 管理介面已設定複雜密碼，**避免使用出廠預設帳密（如 admin/admin、admin/空白）**
- 密碼建議符合以下原則：
  - 至少 **8–12 字元**
  - 含 **大寫、小寫、數字、特殊符號**

【七、電算中心印表機防護處置】

- 強化存取限制：

  防火牆白名單限定 140.115.XX.0/24
- 封鎖攻擊通道：

  停用 TCP 9100（DIPRINT / RAW），僅開啟 LPR（515）、IPP（631）
- 系統更新：

  印表機進行韌體升級 (建議由廠商協助進行)
- 管理介面強化：

  密碼全面更新至至少10碼，含英文大小寫、數字、特殊符號

【七、電算中心印表機防護處置 - HP】

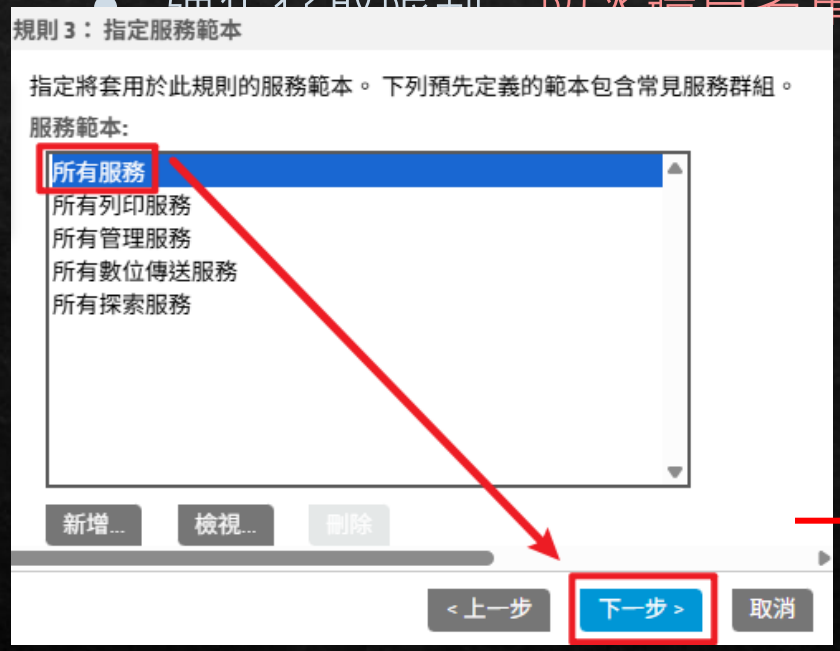
- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

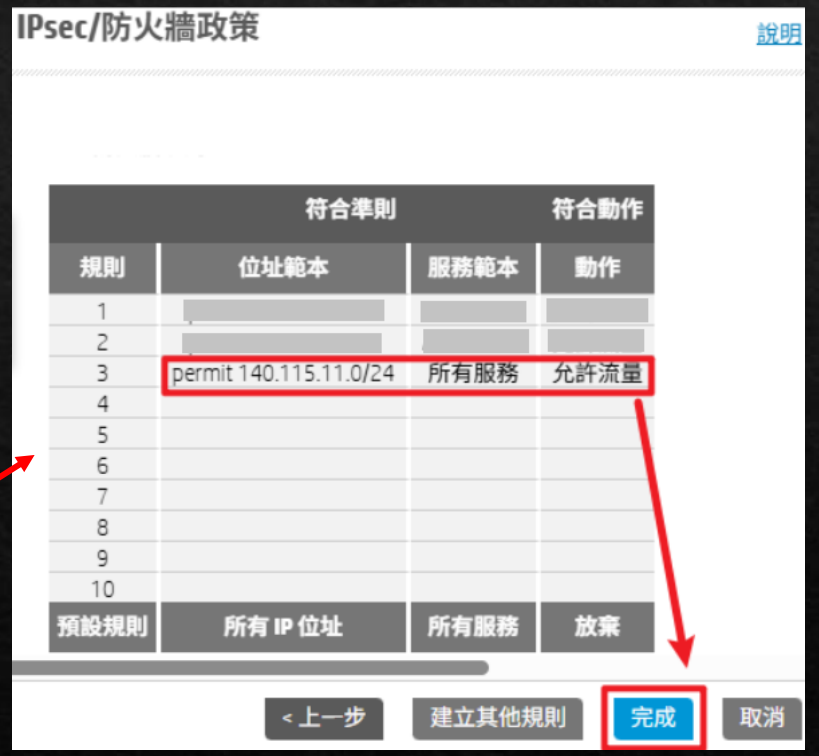
【七、電算中心印表機防護處置 - HP-1】

- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

【七、電算中心印表機防護處置 - HP】

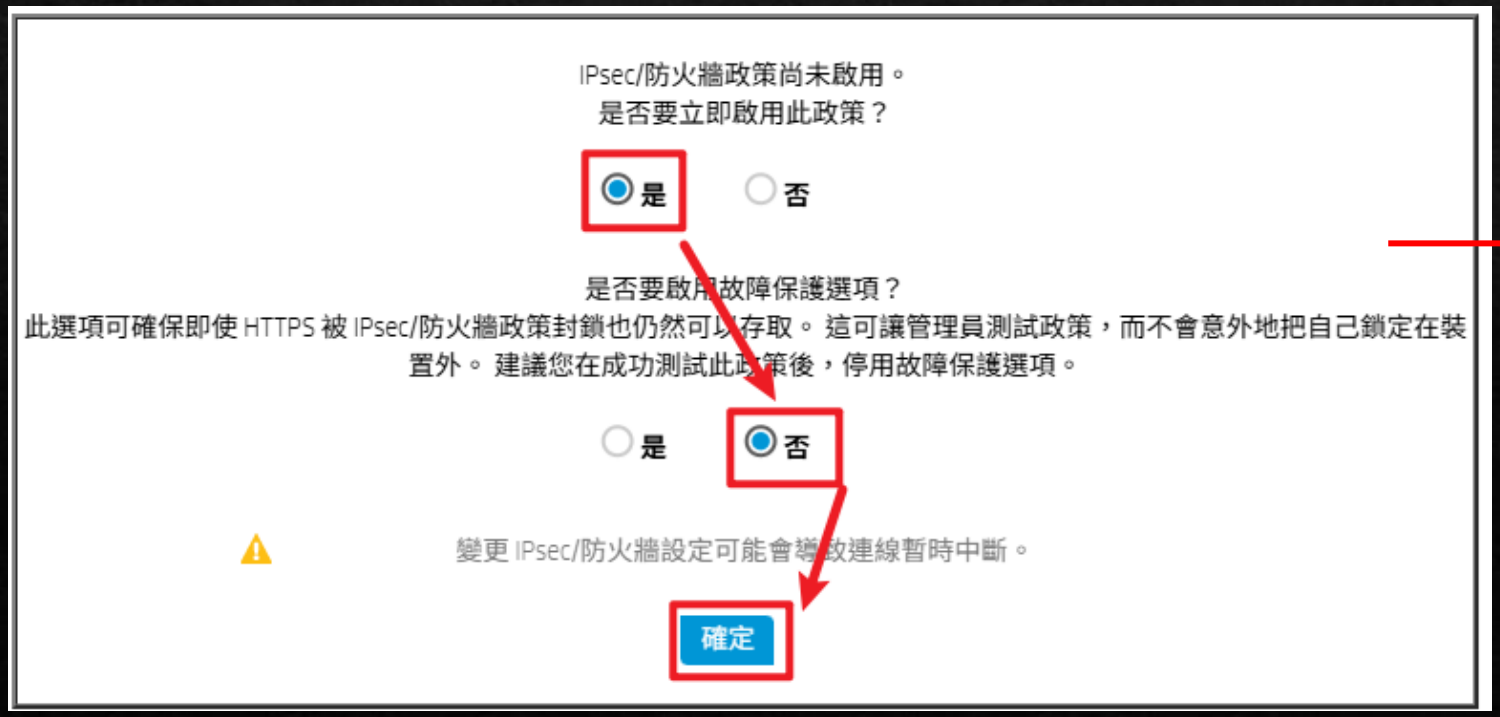
- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

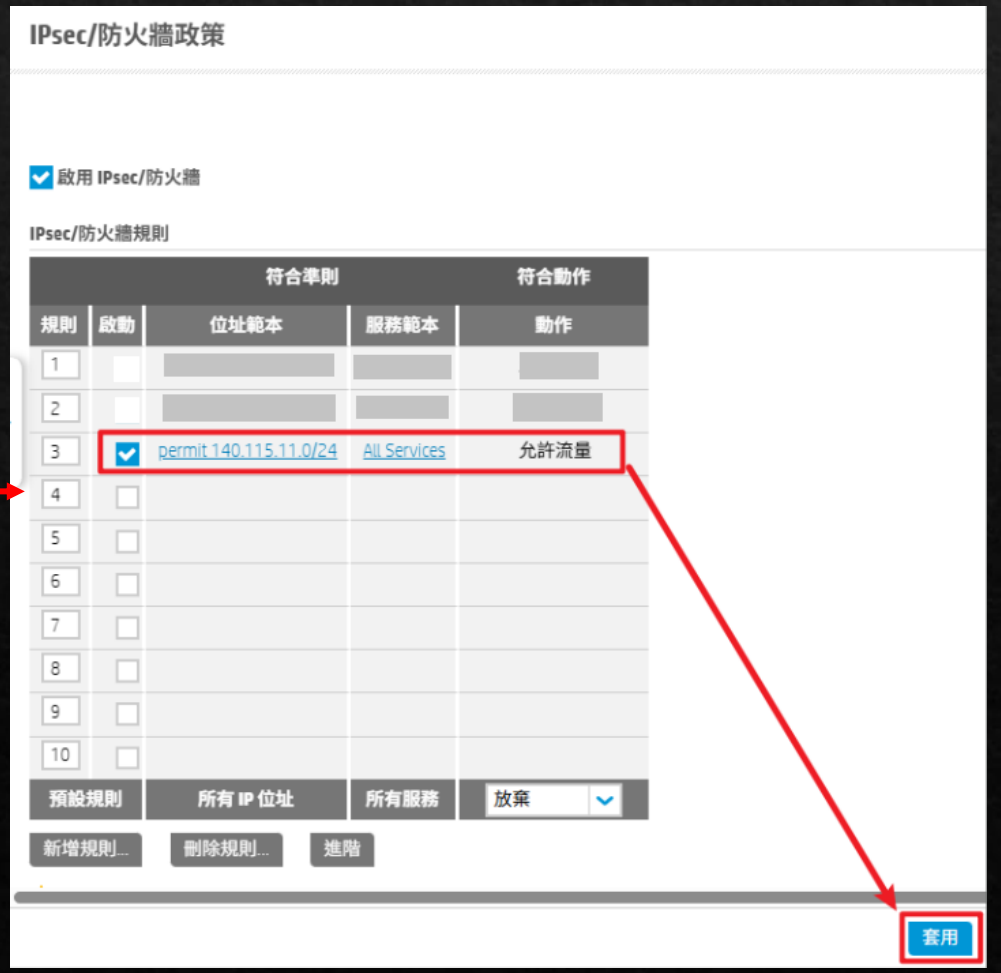




【七、電算中心印表機防護處置 - HP】

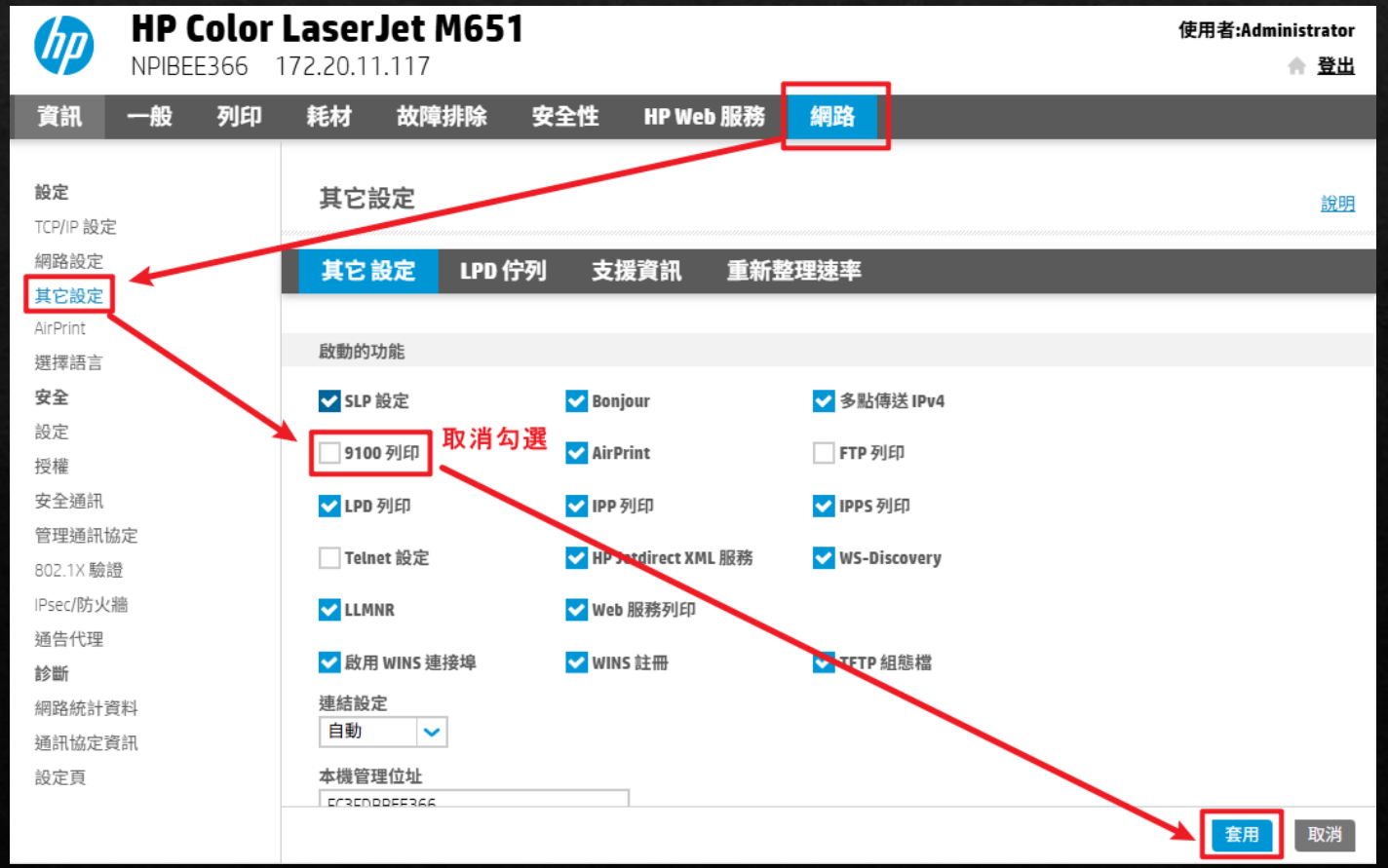
- 強化存取限制：防火牆白名單限定 140.115.XX.0/24





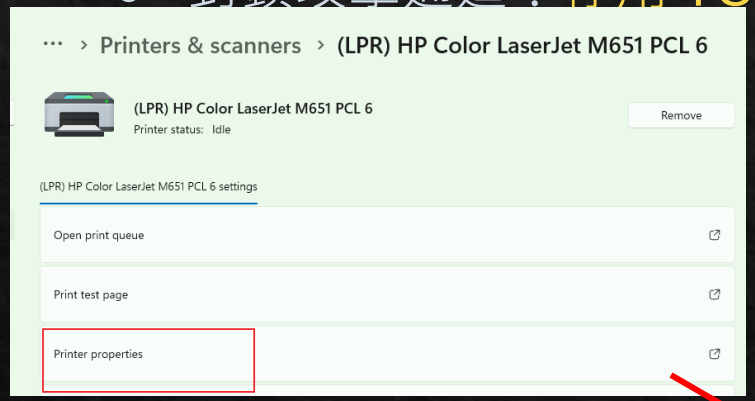
【七、電算中心印表機防護處置 - HP】

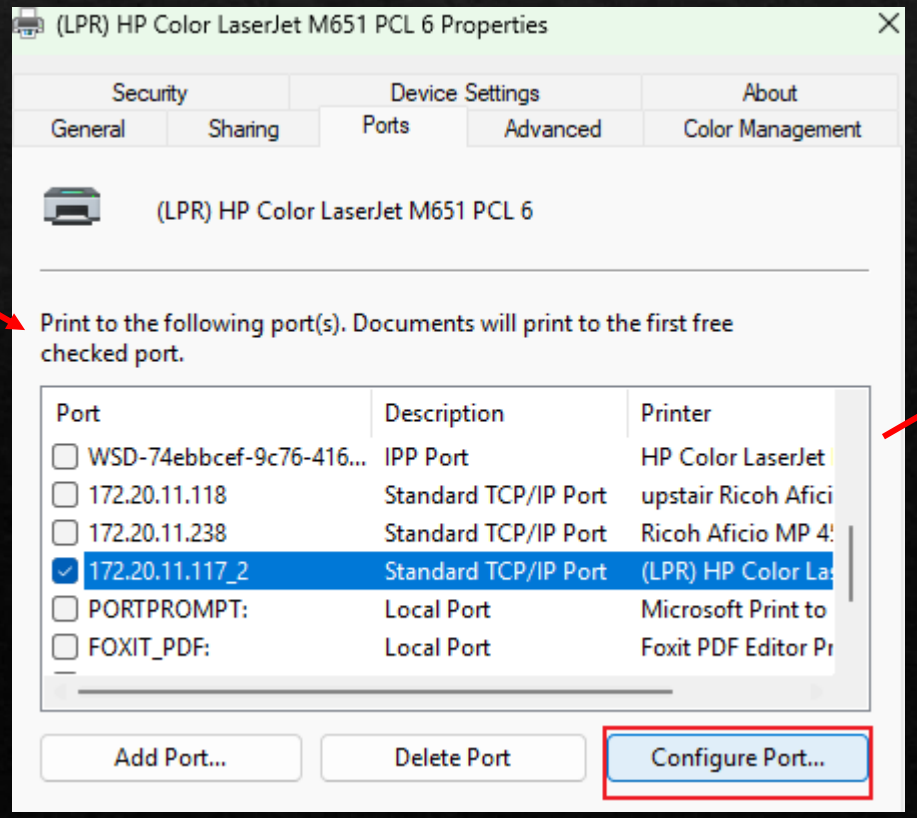
- 封鎖攻擊通道：停用 TCP 9100（DIPRINT / RAW），僅開啟 LPR（515）、IPP（631）

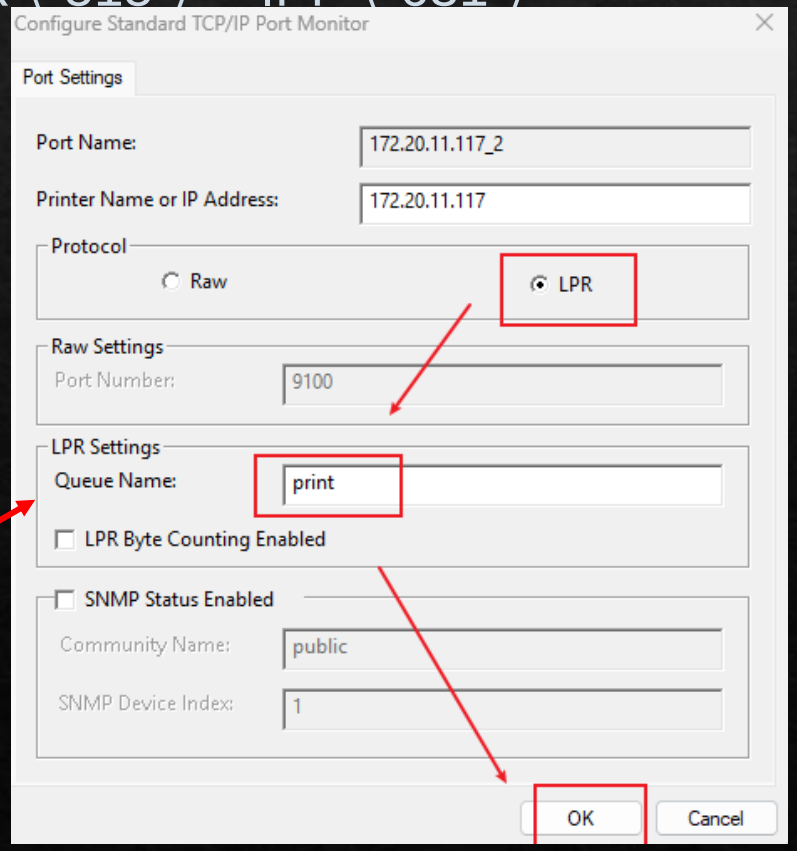


【七、電算中心印表機防護處置 - HP】

- 封鎖攻擊通道：停用 TCP 9100（DIPRINT / RAW），僅開啟 LPR（515）、IPP（631）





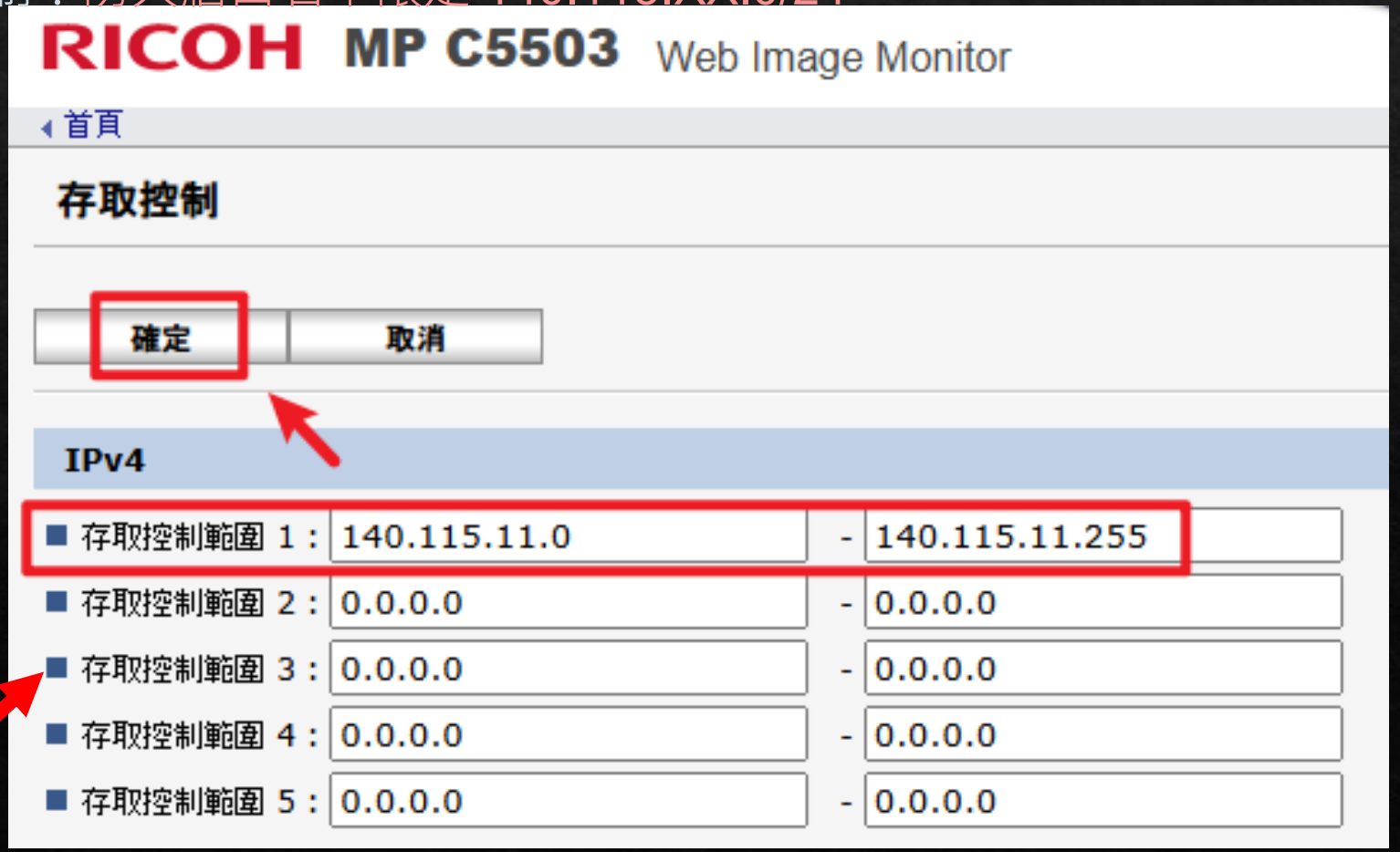


【七、電算中心印表機防護處置 - HP】

- 管理介面強化：密碼全面更新至至少10碼，含英文大小寫、數字、特殊符號

【七、電算中心印表機防護處置 - RICOH】

- 強化存取限制：防火牆白名單限定 140.115.XX.0/24

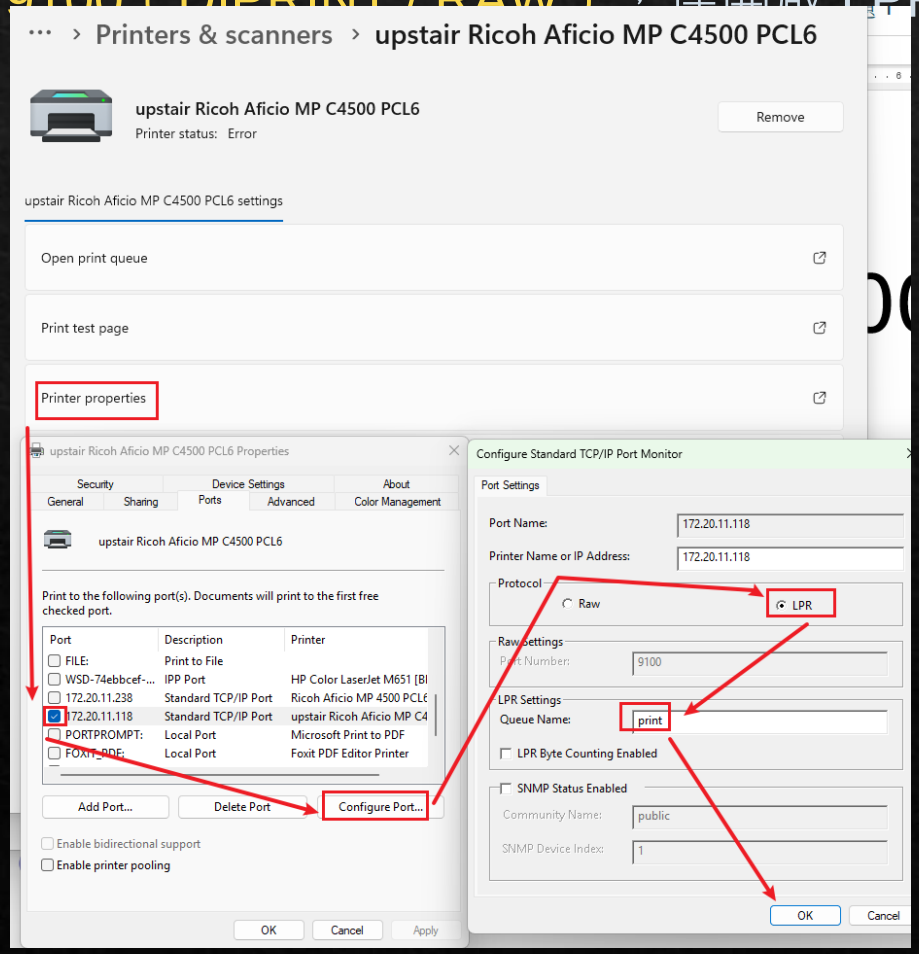


【七、電算中心印表機防護處置 - RICOH】

- 封鎖攻擊通道：停用 TCP 9100（DIPRINT / RAW），僅開啟 LPR（515）、IPP（631）

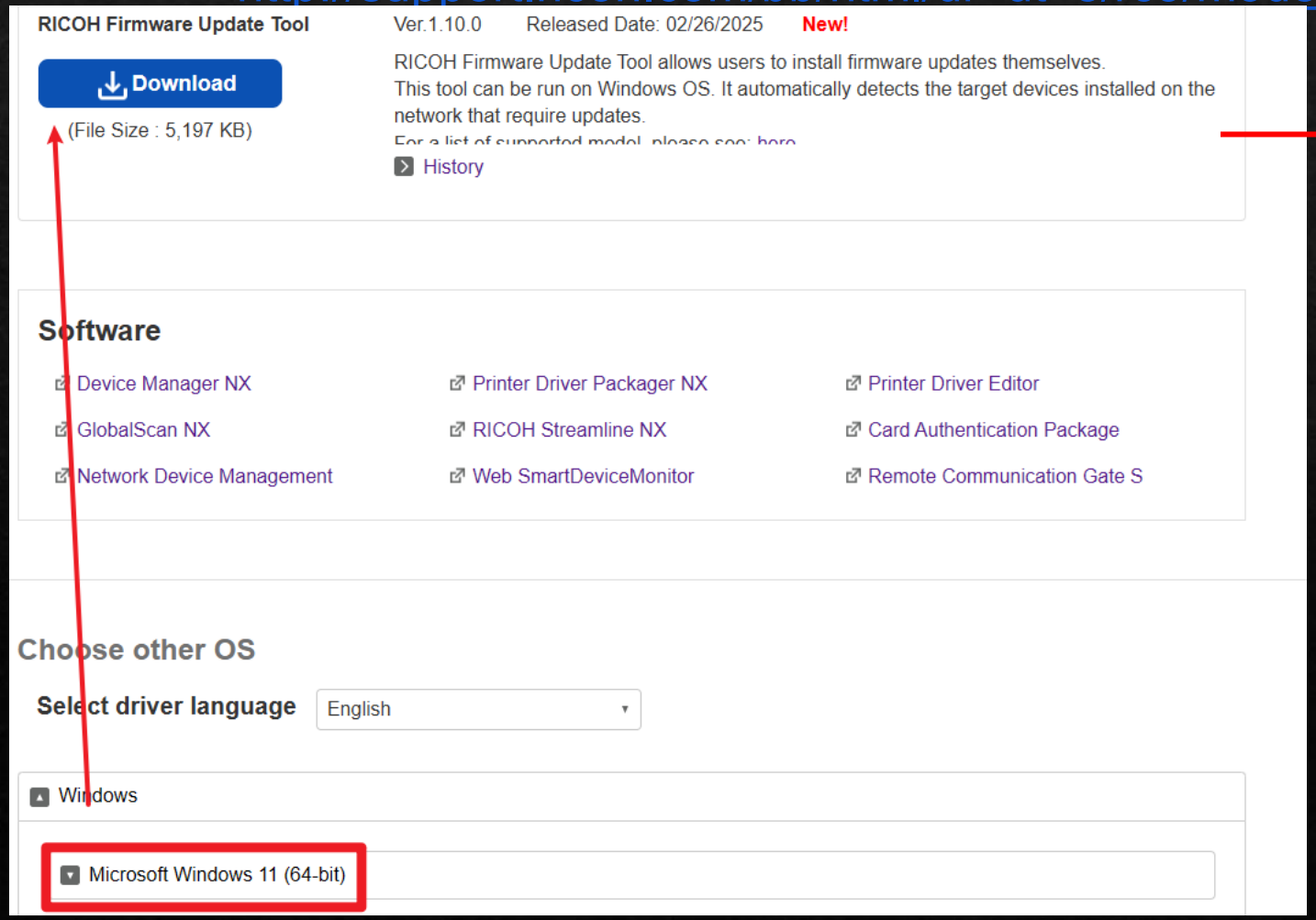
【七、電算中心印表機防護處置 - RICOH】

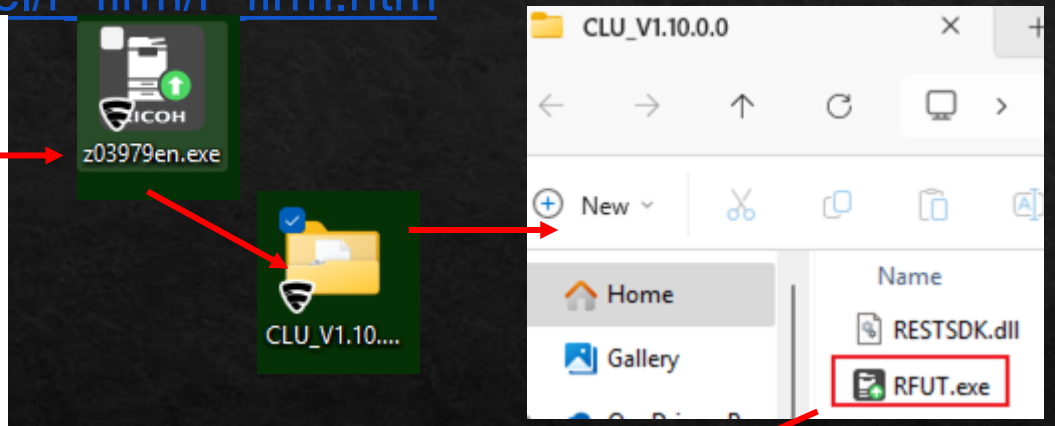
- 封鎖攻擊通道：停用 TCP 9100（DIPRINT / RAW），僅開啟 LPR（515）、IPP（631）

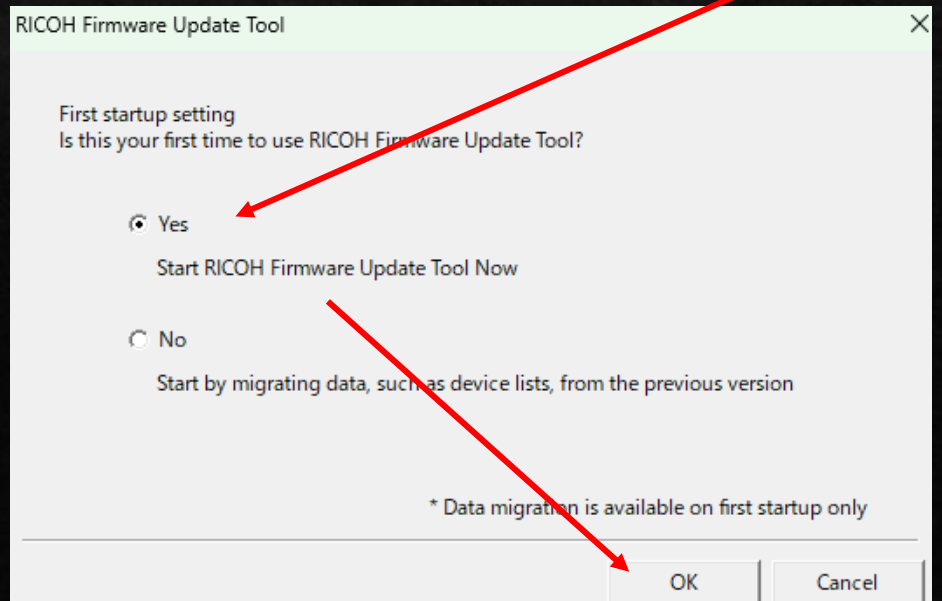


【七、電算中心印表機防護處置 - RICOH】

- 印表機進行韌體升級 (建議由廠商協助進行)
- http://support.ricoh.com/bb/html/dr_ut_e/rc3/model/r_firm/r_firm.htm

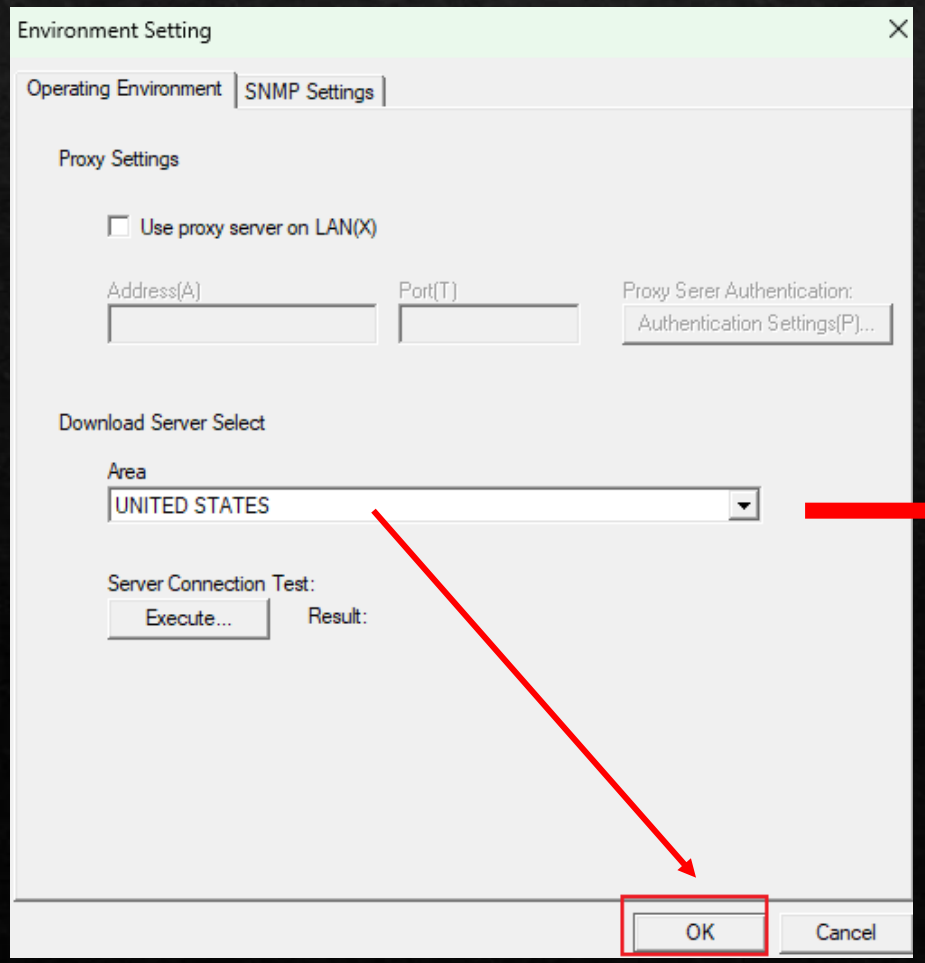


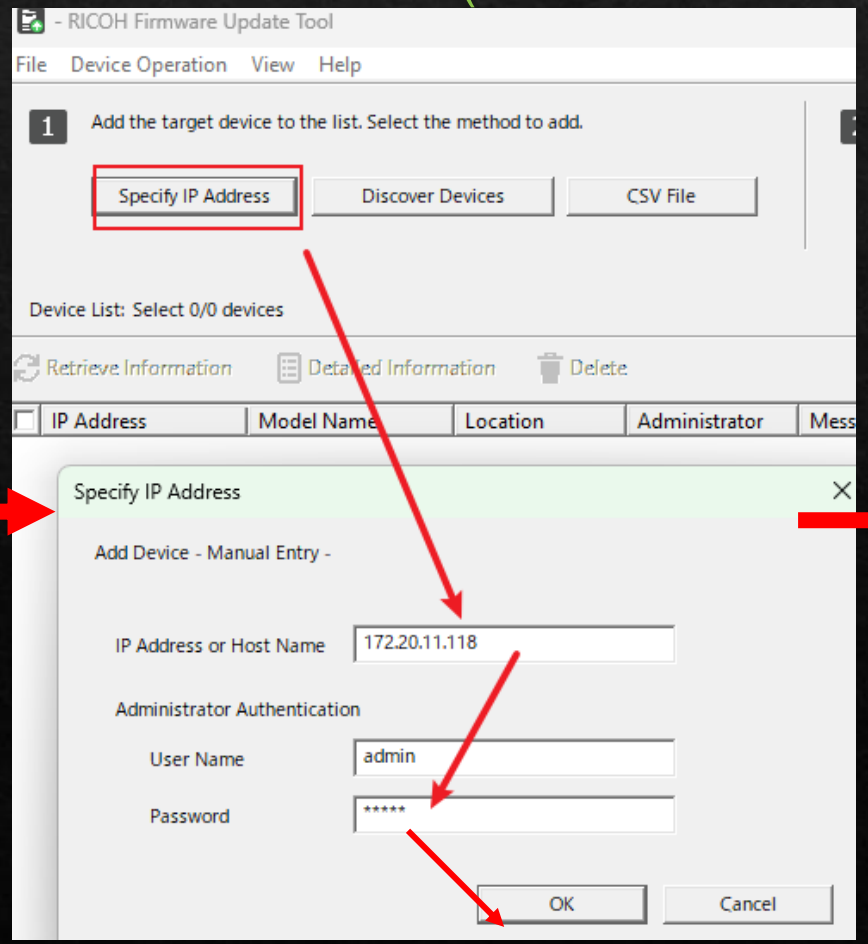


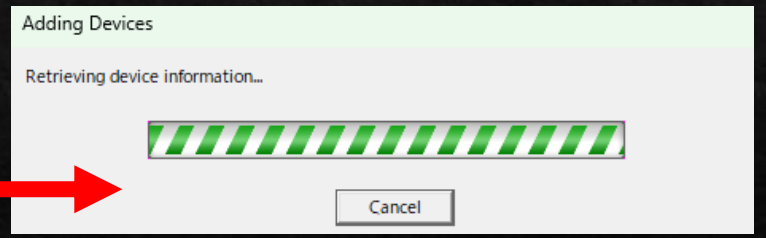


【七、電算中心印表機防護處置 - RICOH】

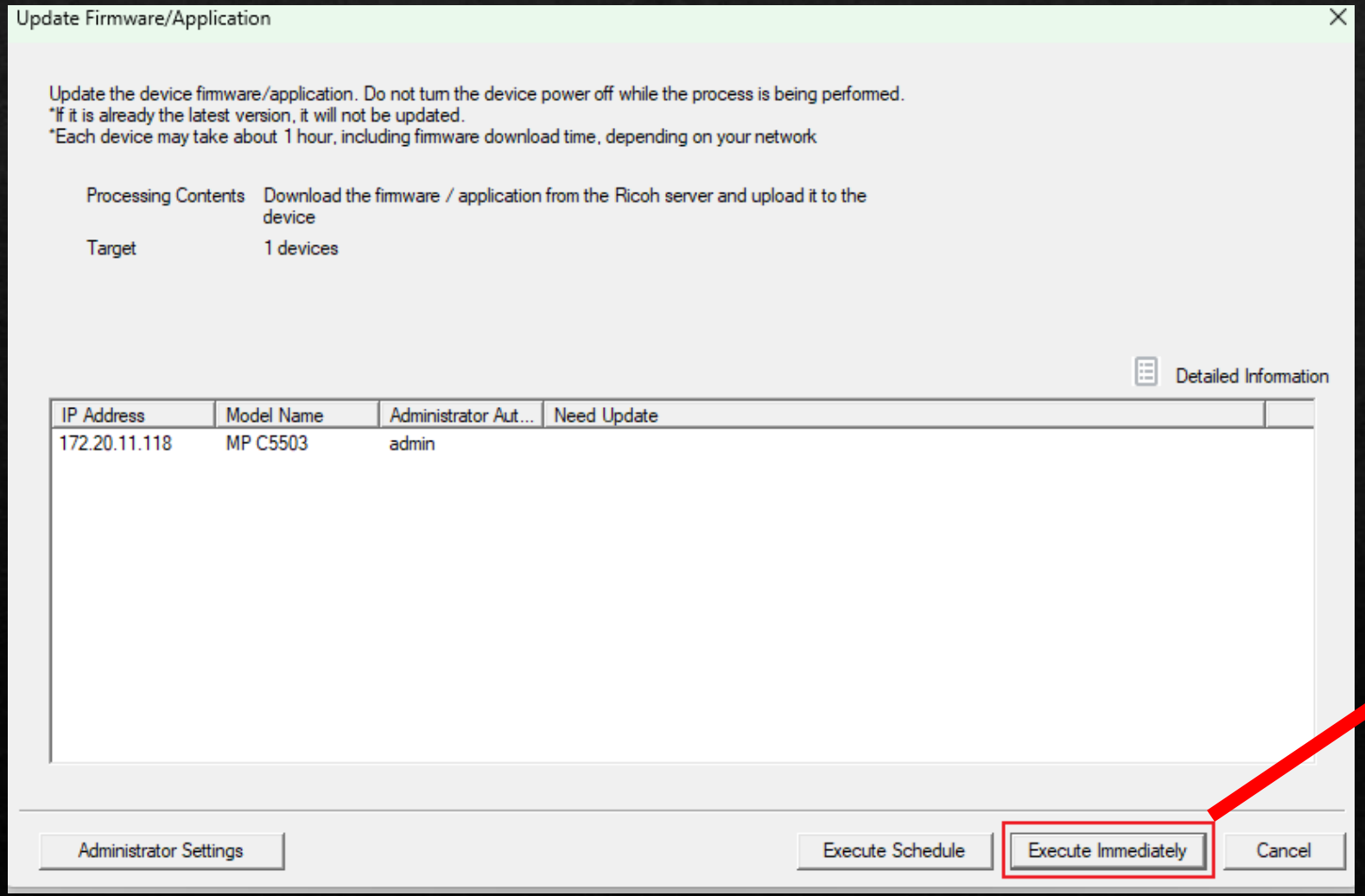
- 印表機進行韌體升級 (建議由廠商協助進行)





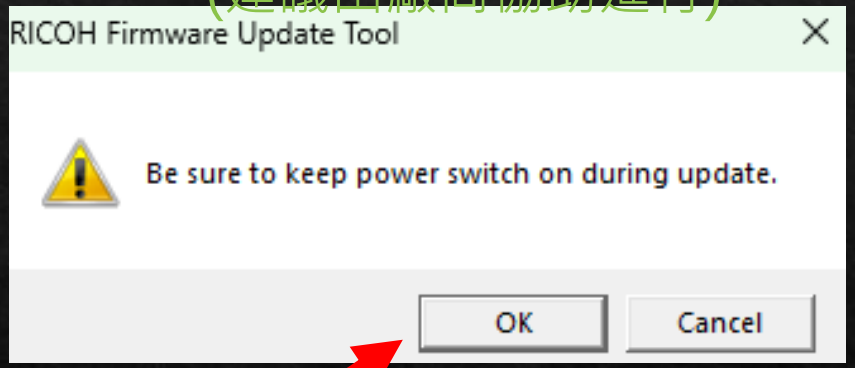


【七、電算中心印表機防護處置 - RICOH】



- 印表機進行韌體升級

(建議由廠商協助進行)



【七、電算中心印表機防護處置 - RICOH】

- 印表機進行韌體升級

(建議由廠商協助進行)

韌體版本 更新前

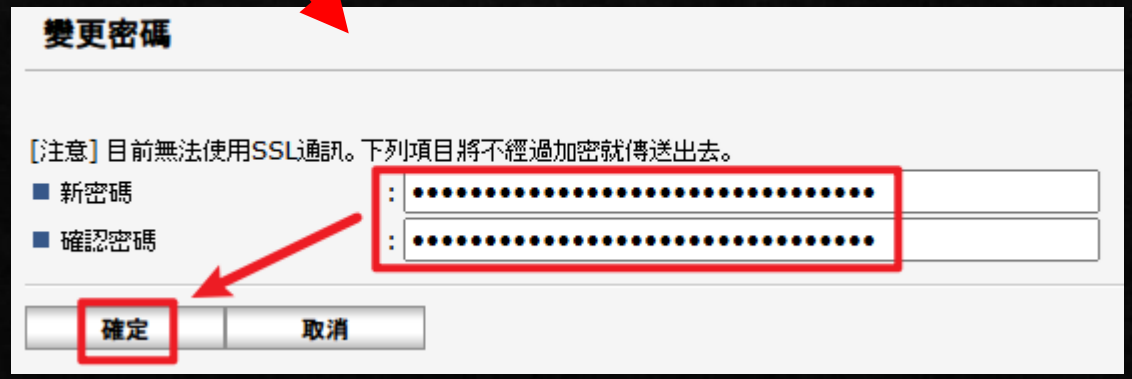
模組名稱	版本	零件編號
System/Copy	1.40	D1495569R
Network Support	12.78	D1495567Y
Font EXP	1.00	D1495581
PCL Font	1.06	D1315586A
PS3 Font	1.12	D6205681
animation	7.00	D1495564D
Fax	15.00.00	D1495557W
RemoteFax	06.00.00	D1495558J
Printer	1.20	D1665701X
RPCS	3.13.24	D1665703F
PCL	1.20	D1665706R
PDF	1.05	D1665733F
Scanner	01.16	D1495560T
NetworkDocBox	1.05	D1495568G
Web Support	1.04.9	D1495561M
Web Uapl	1.04.4	D1495562G
Java VM v11 std	11.28.03	D1495579Q
PS3	1.00	D1665731A
Data Erase Onb	1.01x	D3775934
GWFCU3.8-2(WW)	11.00.00	D1495559M
PowerSaving Sys	F.20	D1495554E
Engine	1.39:08	D1505504C
OpePanel	1.09	D1491490K
LANG0	1.09	D1491490K
LANG1	1.09	D1491490K
ADF	01.340:16	D6835550F

韌體版本 172.20.14.118 更新後

模組名稱	版本	零件編號
System/Copy	1.47	D1495569Y
Network Support	12.83	D1495565B
Font EXP	1.00	D1495581
PCL Font	1.06	D1315586A
PS3 Font	1.12	D6205681
animation	7.00	D1495564D
Fax	15.00.00	D1495557W
RemoteFax	06.00.00	D1495558J
Printer	1.24	D1665708A
RPCS	3.13.24	D1665703F
PCL	1.20	D1665706R
PDF	1.06	D1665733G
Scanner	01.17	D1495560V
NetworkDocBox	1.11	D1495568N
Web Support	1.13	D1495561Y
Web Uapl	1.07	D1495562L
Java VM v11 std	11.28.03	D1495579Q
PS3	1.00	D1665731A
Data Erase Onb	1.01x	D3775934
GWFCU3.8-2(WW)	11.00.00	D1495559M
PowerSaving Sys	F.20	D1495554E
Engine	1.43:08	D1505504G
OpePanel	1.09	D1491490K
LANG0	1.09	D1491490K
LANG1	1.09	D1491490K
ADF	01.340:16	D6835550F

【七、電算中心印表機防護處置 - RICOH】

- 管理介面強化：密碼全面更新至至少10碼，含英文大小寫、數字、特殊符號



【八、結論與建議】

本事件屬於內部主機遭入侵後，向內網其他設備進行橫向滲透之案例。

本次攻擊行為特徵顯示，懷疑是自動化掃描器（如 masscan、nmap、zgrab）誤將印表機 9100 埠誤認為一般 TCP 服務，套用通用 HTTP 攻擊 payload 進行攻擊，導致印表機列印異常資料。

雖攻擊者未必意識到目標為印表機，但此舉仍暴露出內網存取控管與設備防護的不足，提供了一次檢視現有防護機制的契機。

- 後續建議：
    - 優先落實來源 IP 存取限制，有效縮小內網暴露面。


THANK YOU
BEARY MUCH!