

網路印表機自動列印勒索文件相關說明

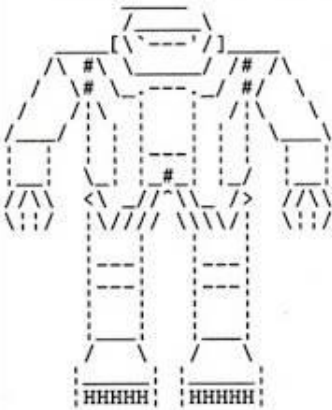
1. 現象說明:

近期各廠牌網路印表機經常被客戶反映會自動印出“ Your Printer has been owned” 或勒索比特幣(BitCoin)的恐嚇文件，針對此問題Epson印表機提供相關處理及因應方式如下，關於其他廠牌印表機所出現的類似問題可洽詢各廠牌所屬客服之協助。

*恐嚇文件內容:

```
READ -->
-----
stackoverflowin has returned to his glory,
your printer is part of a botnet,
the god has returned,
everyone likes a meme,
fix your bullshit.

overflow at:
(WORD) = ((struct Elf32_Ehdr*)((0xFF & memes)base)->e_machine)
-----
Email: sthacker@protonmail.com
Twitter: https://twitter.com/lmaostack
stackoverflowin has returned to his glory,
your printer is part of a flaming botnet,
the hacker god has returned from the dead.
----> YOUR PRINTER HAS BEEN OWNED <----
```

A person-shaped ASCII art made of dashes, with a hat on top and feet at the bottom. The body consists of a series of connected dashes forming a torso and limbs. There are some symbols like '#' and '<' integrated into the art.

```
((struct Elf32_Ehdr*)((0xFF & memes)base)->e_machine)
-----
Email: stackoverflowin@tuta.io
Twitter: https://twitter.com/lmaostack
-----
GREETINGS FROM BREAKTHEINTERNET (BTI) WITH LOVE
```

2. 問題分析:

- A. 駭客透過連接埠 9100 傳送 ASCII 字元使印表機印出恐嚇或勒索文件。
- B. 此問題僅發生在當印表機直接連接到網際網路或是設定在公開的網際網路 IP 位址而前端沒有防火牆保護的情況下。

3. 危害釋疑:

因為印表機的連接埠9100僅能接收列印資料，故印表機並無法執行列印以外的其他工作。
此外印表機並不會因此而發生故障、資料洩漏或是印表機被控制的情形。

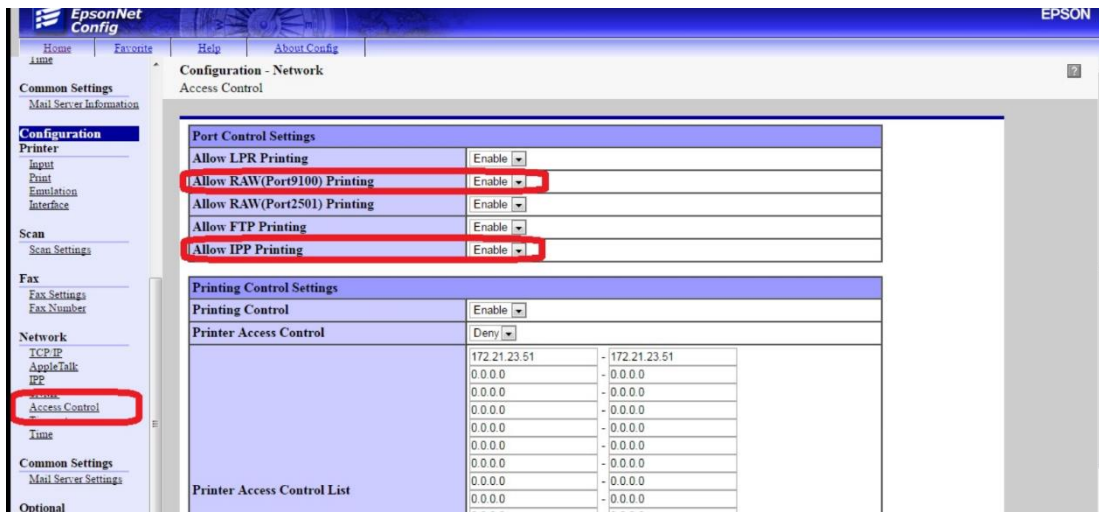
* 僅就目前現有案例進行分析，若有其他類似文件由印表機印出依然有可能為PC端被植入木馬而產生之遠端列印，故請同時確認相關之網路環境安全。

4. 處理方式:

- a. 為了防止駭客不正當的存取網路印表機，我們強烈建議使用者重新檢視防火牆端的安全設置。
- b. 請確認印表機所連接的網路環境是否都受到防火牆的保護，若未受保護請盡快調整至適當的配置。
例如:使用具備安全功能的路由器/啟用路由器中的防火牆設定。
- c. 透過 EpsonNet Config 關閉印表機端連接埠 9100 改由透過 LPR 列印，請於瀏覽器輸入列表機 IP 位置後請參考下列步驟進行相關設定。

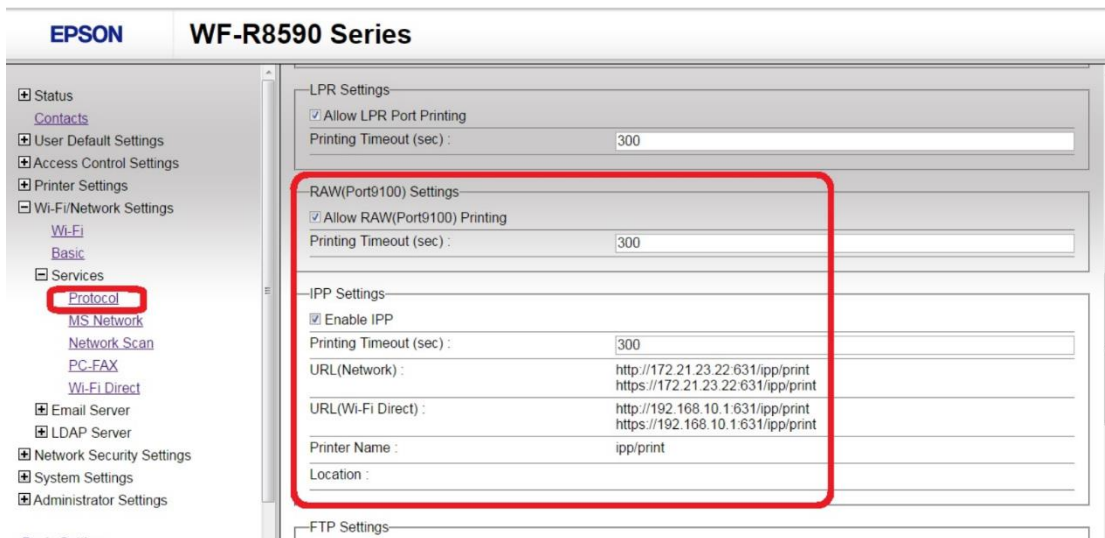
雷射印表機設定畫面:

- Configuration=>Network=>Access Control=> 1. Allow RAW(Port9100)Printing=Disable
2. Allow IPP Printing= Disable.



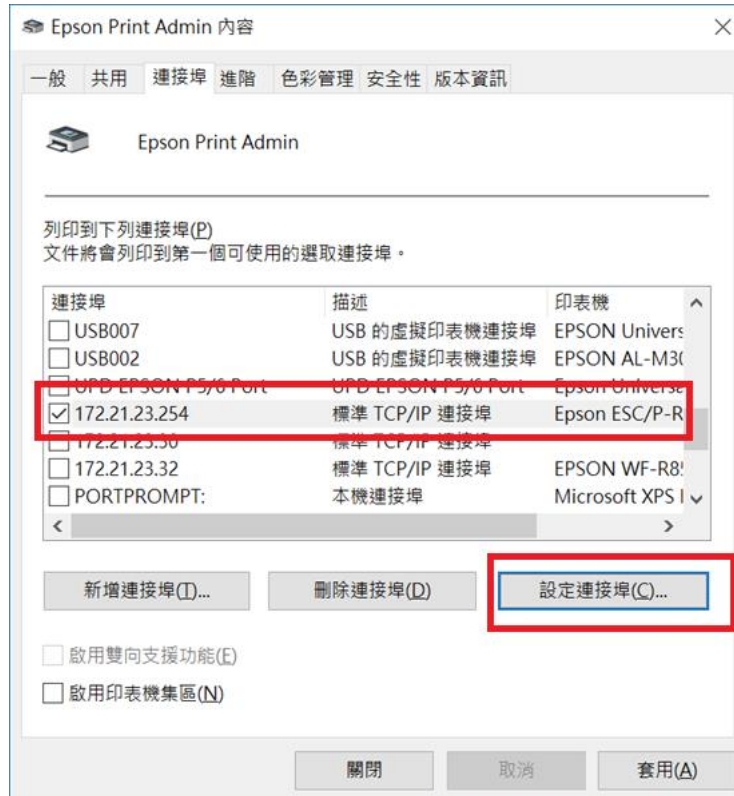
噴墨印表機設定畫面:

- Service=>Protocol=>1. 取消勾選Allow RAW(Port 9100)Printing。
2.取消勾選Enable IPP。



驅動程式端的調整:

a. 選擇印表機的 IP 位置 => 點選“設定連接埠”



b. 通訊協定由原始(連接埠 9100)變更為 LPR 列印後按下確定即完成設定。

