個案分析-

網路印表機之比特幣勒索信事件事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106 年 4 月

I. 事件簡介

1. 殭屍網路 Mirai 於 2016 年 9 月現身之後，造成全球網路世界開始發生好幾起大規模 IoT 設備的 DDoS 攻擊事件，最高攻擊流量甚至超過 1Tbps。
2. 接著 2017 年 2 月中開始，陸續有許多學校的網路印表機收到駭客恐嚇信，要求支付 0.05 和 3 BTC 不等的比特幣，引起相關單位對 IoT 設備資安的高度重視。
3. 本次事件為某學校有一台網路印表機，大量收到要求支付 0.05 BTC 給駭客的恐嚇信造成使用者困擾，而該設備型號為「Fuji Xerox DocuPrint P455 d」。

4. 此恐嚇信內容很簡短，只表示該設備已經被駭入，並支付 0.05BTC 到錢包地址。

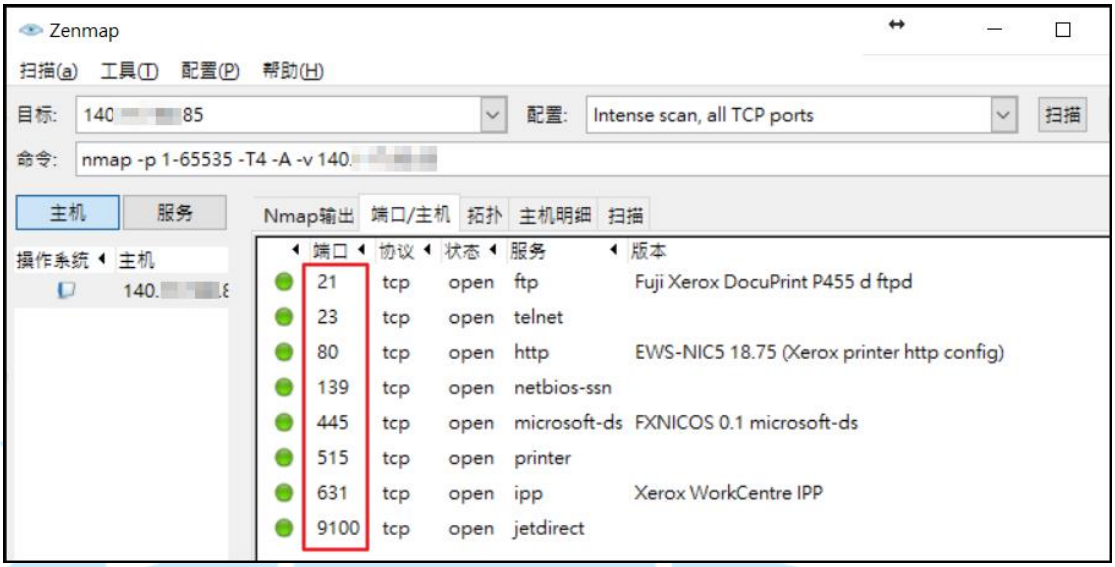
```
Hacked: Please send 0.05 Bitcoin to 1DgjttwnDVgCbDfRFgb4siU4hcrN1HY1VW
```

5. 該印表機使用者表示，當初安裝時候完全沒有做過任何設定，就連 IP 都是使用 DHCP 取得的 public IP，所以成為被駭入目標。

II. 事件檢測

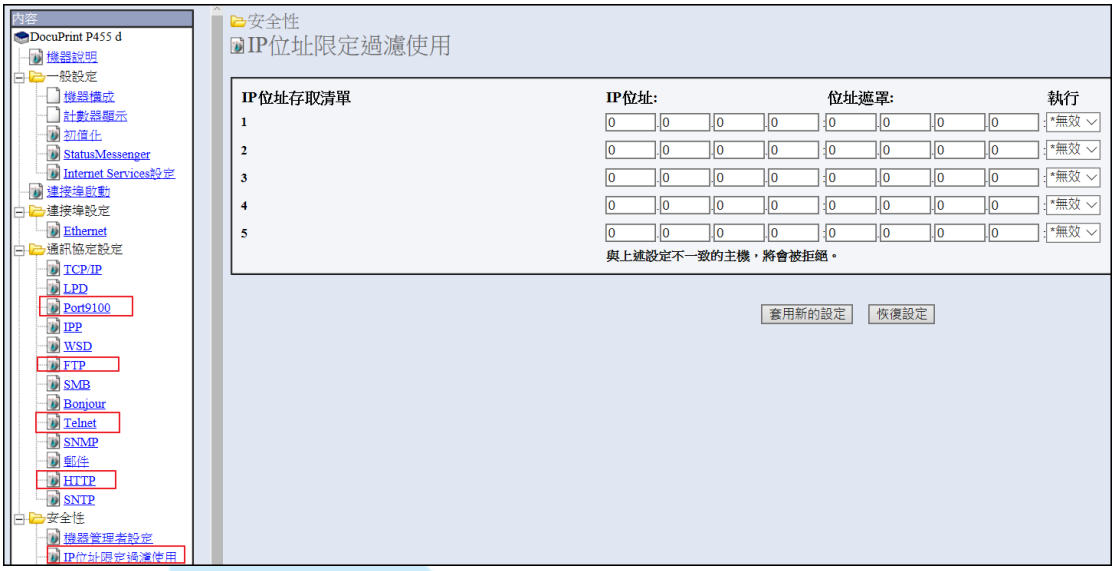
1. 根據最近調查到許多學校遭駭的印表機廠牌以 HP 比例 73%為最大宗，然而此事件設備廠牌為 Fuji Xerox，表示不論廠牌大小都有可能被入侵。

2. 首先透過 NMAP 對該設備進行 port scan，發現到印表機預設開啟許多 PORT，主要有 port 21、23、80、9100 等常用通訊埠。



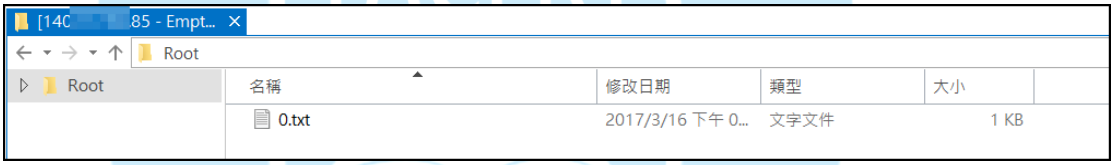
3. 首先檢查 port 80 的網頁服務頁面，發現該網頁並無登入權限設定，任何人都能夠輕易存取網頁管理頁面。在列印使用者限制權限方面，並無設定任何限制，導致任何網段 IP 都能夠存取到印表機。

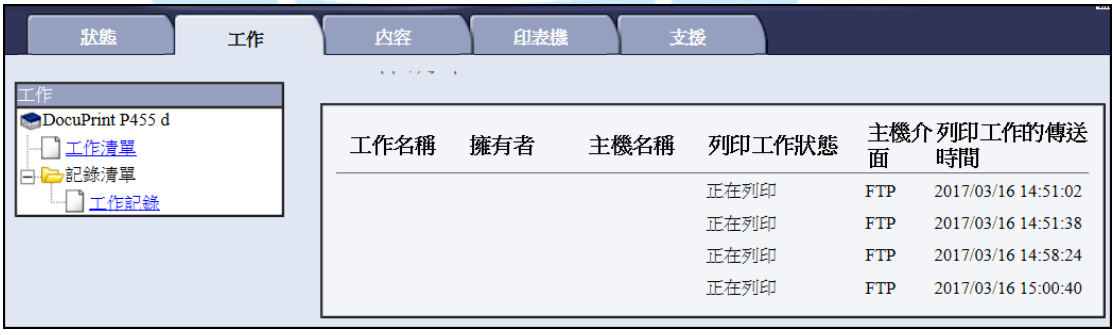
4. 接著查看網站內容部分，裡面都是印表機組態設定功能項目，包含通訊協定設定和安全性設定等，其中以安全性設定最為重要有 ACL 功能，不過並無特別設定。



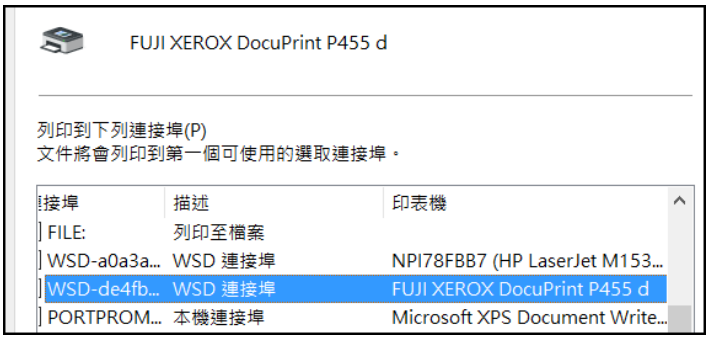
5. 在檢查 HTTP 服務功能中，並無直接上傳檔案列印功能，因此檢查 FTP 服務，發現能夠輕易以匿名帳號登入 FTP 服務。

6. 在登入 FTP 後，預設根目錄為 Root 資料夾，並且能夠上傳任意檔案。測試上傳一個文字檔 0.txt，該檔案傳輸完成後就會被自動清除，在檢查 Web 的工作頁面可以看到文件正在列印中的顯示。





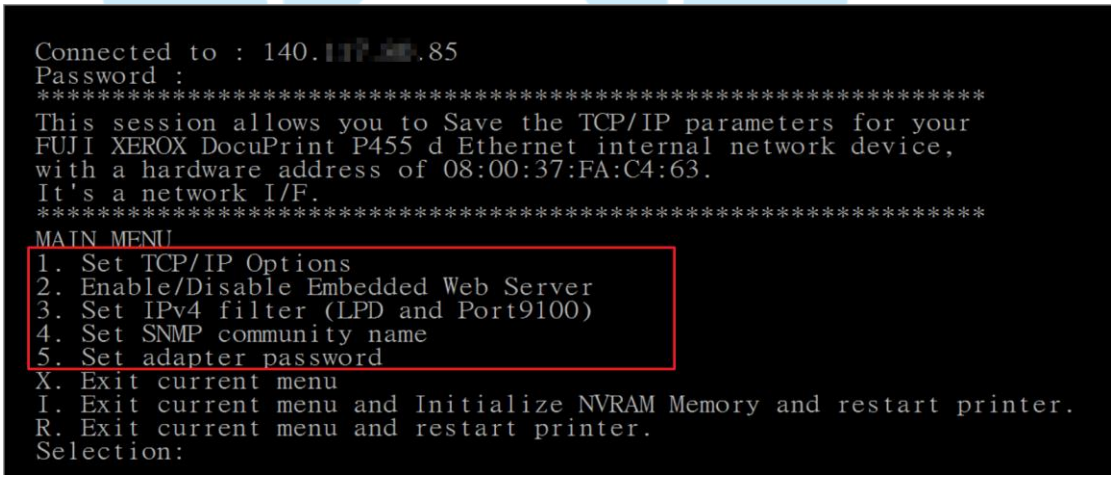
7. 此外透過作業系統新增印表機也能跨網段將該印表機加入連線，如此一來更容易將恐嚇信透過 port 9100 方式將恐嚇信列印出。



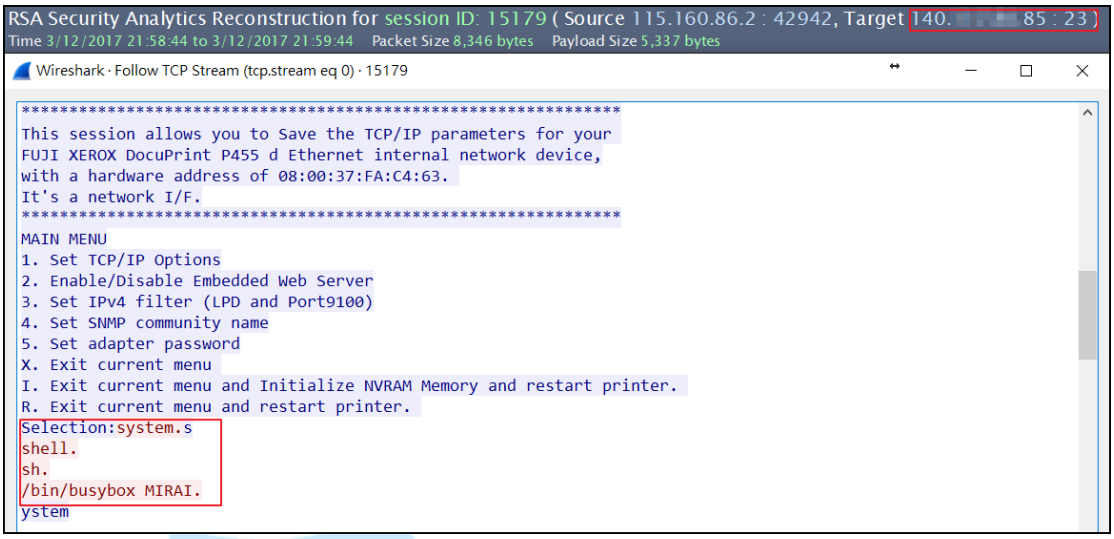
8. 檢查 WEB 介面的列印工作紀錄，發現在 3/5 期間有大量透過 port 9100 列印的紀錄，符合當時列印出恐嚇勒索信的時間。

工作名稱	擁有者	主機名稱	列印輸出	頁數	主機介面	列印工作的傳送時間
			正常結束	1	Port9100	2017/03/05 11:10:08
			正常結束	1	Port9100	2017/03/05 11:12:27
			正常結束	1	Port9100	2017/03/05 11:14:55
			正常結束	1	Port9100	2017/03/05 11:17:38
			正常結束	1	Port9100	2017/03/05 11:20:07
			正常結束	1	Port9100	2017/03/05 11:22:32
			正常結束	1	Port9100	2017/03/05 11:25:01
			正常結束	1	Port9100	2017/03/05 11:27:33
			正常結束	1	Port9100	2017/03/05 11:30:02

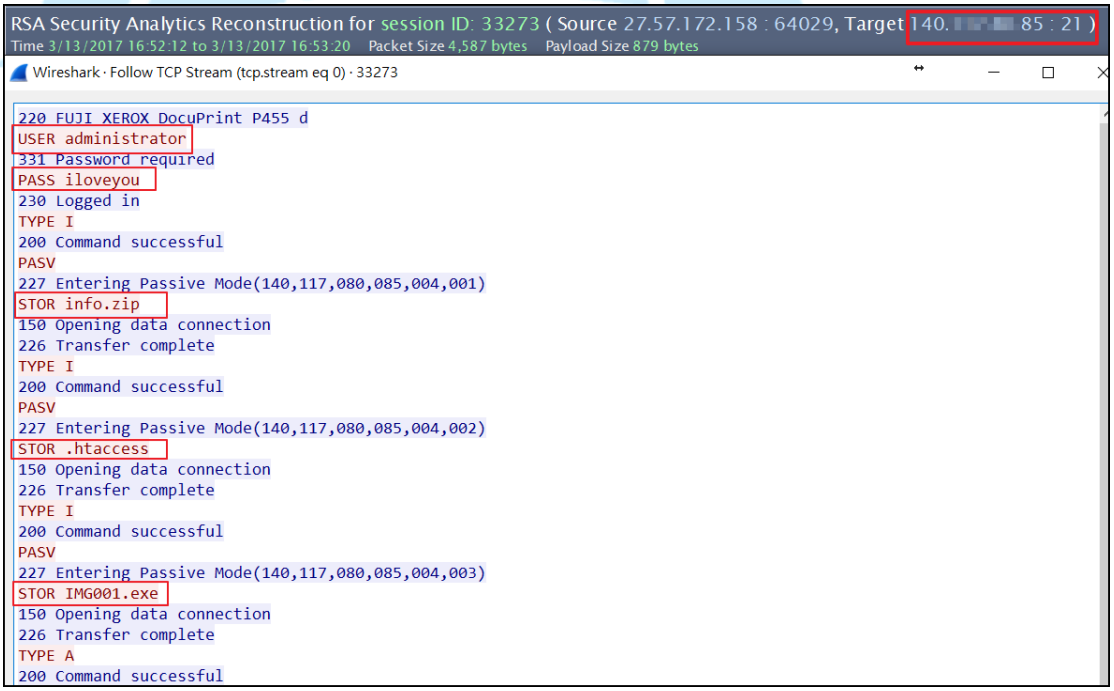
9. 此外測試 port 23 的 telnet 連線，也能夠輕易成功登入，因為預設的密碼為空。在此雖無法直接列印文件，但是能夠對網路相關組態進行設定，包含 IP 和 ACL 設定等。



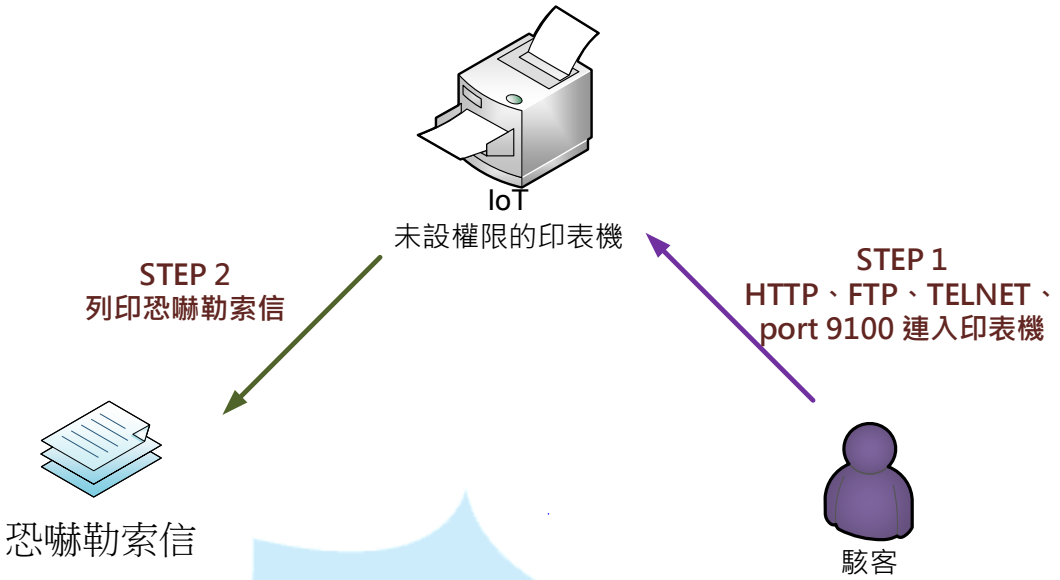
10. 接著分析側錄的封包發現，有大量的外部 IP 針對印表機的 TELNET 和 HTTP 服務進行連線，其中一筆韓國 IP 115.160.86.2 成功連入印表機的 TELNET 後，嘗試執行 shell 指令及測試是否為 MIRAI botnet，然而該介面無法回應 shell 指令執行。



11.接著檢查封包發現有 IP 27.57.172.158 成功連入 FTP 服務，並且嘗試上傳 ZIP 檔、執行檔和其他檔案來植入後門惡意程式，研判駭客也有可能繞過 port 9100 使用 FTP 方式列印恐嚇勒索信。



III. 網路架構圖



Step 1: 駭客從 Internet 透過 port 9100 或 FTP 連入網路印表機。
Step 2: 印表機收到駭客上傳的文件後列印出恐嚇勒索信要求支付贖金0.05BTC。
Step 3: 必須啟動印表機的防護機制，以免遭外人惡意利用。

IV.建議與總結

1. 此事件為物聯網設備 IoT 遭駭客入侵利用所致，主因是該設備並無設定防護機制遭駭客利用列印恐嚇勒索信。
2. 駭客可以透過 FTP 及 port 9100 直接存取印表機列印文件，故以亂槍打鳥方式隨意發送恐嚇勒索信要求支付 BTC 贖金。
3. 因此該設備除了阻擋 port 9100 之外，FTP 也是可能被入侵的管道。
4. 印表機的 TELNET 和 HTTP 服務並未關閉和限制，可能遭駭客串改印表機的網路設定等。
5. 解決方式可以設定印表機的 ACL 規則，限制外部網段無法存取，或者將 IP 設定為內部虛擬 IP，避免直接暴露在 Internet 中。
6. 另一種解決方式不用改為虛擬 IP，但是要把印表機的閘道 IP 給清空，阻斷到 Internet 的通道。

V. 相關報導

1. http://www.ithome.com.tw/news/111674

2. http://www.ithome.com.tw/news/112300

3. http://www.ithome.com.tw/news/112282

iThome

比特幣集體勒索又來了，這次鎖定全臺4千校！不只大學，桃園3小學也出現駭客勒索信

桃園市有3所中小學近日收到駭客恐嚇信，揚言若不支付比特幣，就會在3月1日癱瘓學校網路。此外，也有部分大學同樣收到駭客威脅信。駭客利用連線印表機的公開IP和預設密碼，侵入學校網路列印。

文/ 黃泓瑜 | 2017-02-22 發表

讚 3.9萬 按讚加入iThome粉絲團 讚 2,272 分享 G+1 5