個案分析-

HP 印表機資訊頁面置換

TACERT 臺灣學術網路危機處理中心團隊製

2012/1

HP 印表機資訊頁面置換事件分析

一、事件發生時間：

2011 年 12 月 26 日　教育機構資安通報平台派發網頁置換事件單

二、事件通報單位：

系統安全及反駭客團隊(國立清華大學)

三、事件分類：

DEF 網頁置換

四、事件影響範圍：

當日發現 5 所學校共 8 台印表機資訊頁面遭駭客置換頁面

五、事件說明：

(一) 當日上午系統安全及反駭客團隊透過教育機構資安通報平台派發共 8 張網頁置換事件單。

事件單派發後，接獲轄下單位反應事件單內容派發有問題疑似誤報。經確認原舉報單位提供之佐證資料，確實為網頁置換事件非誤報，並檢查確認其他相關事件單，發現此攻擊行為。

（二）相關佐證資料：

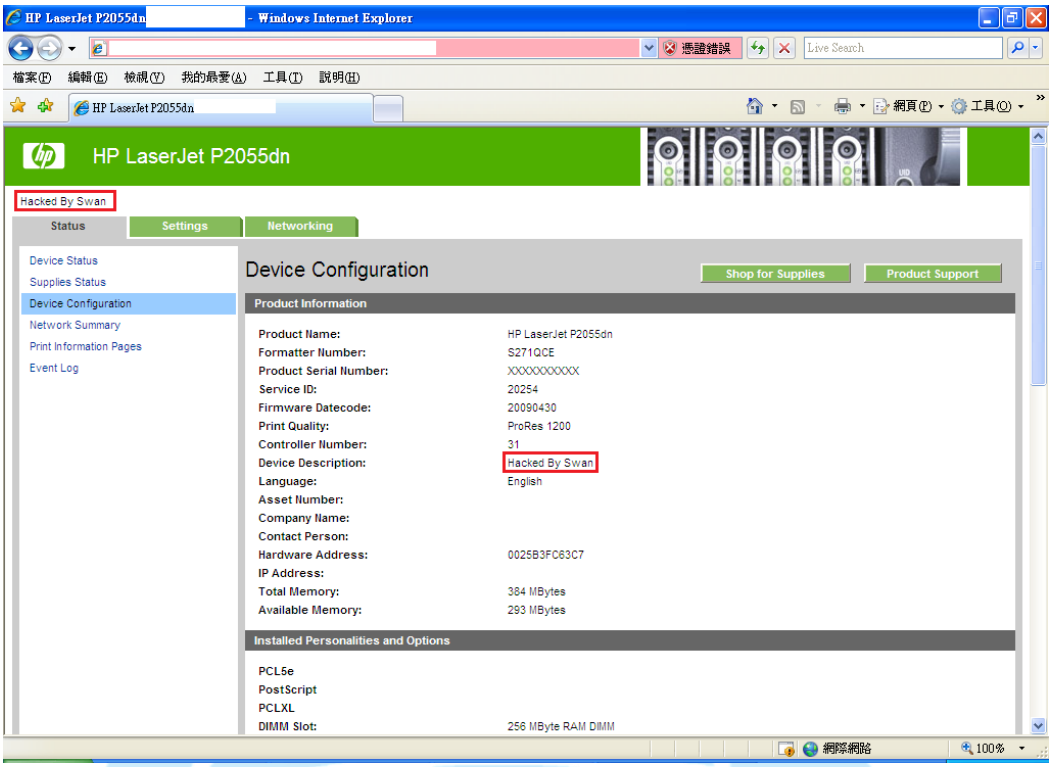

圖 1. 受害印表機資訊頁面畫面(圖片由系統安全及反駭客團隊提供)

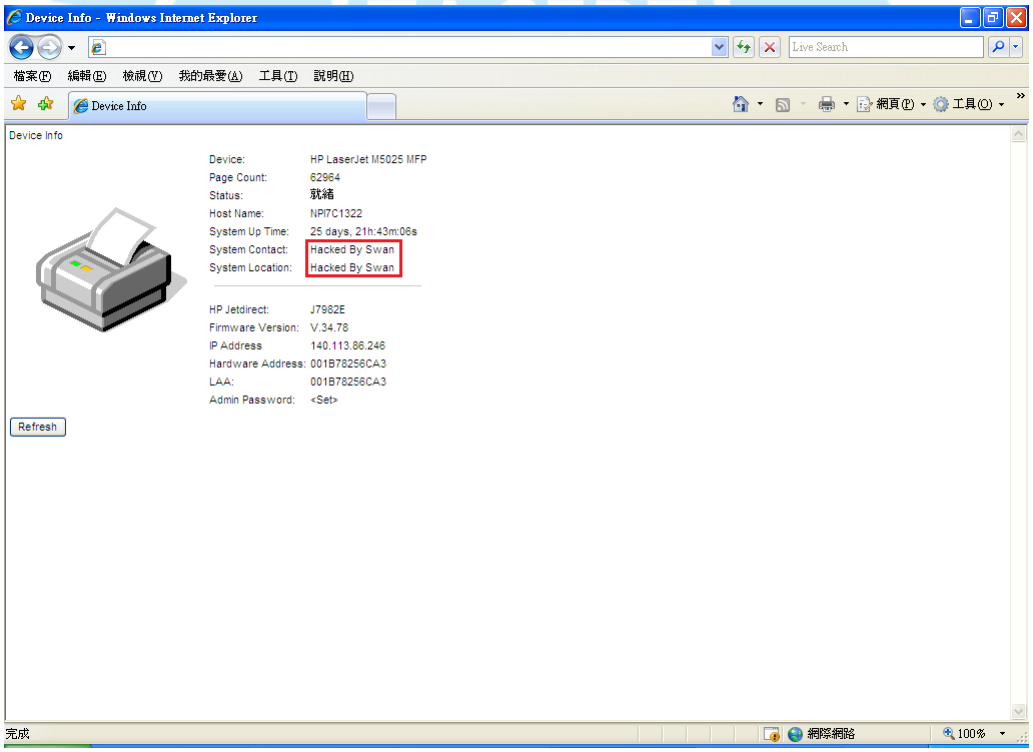

圖 2. 受害印表機資訊頁面畫面(圖片由系統安全及反駭客團隊提供)

六、分析結果：

(一)由圖 1 及圖 2 可發現此網頁置換事件所置換資訊皆為「Hacked By Swan」，應為同一組織或人員所為。

(二)由圖 1 及圖 2 可發現此網頁置換事件所受害印表機皆為 HP，且皆有網頁管理功能。

(三)進行相關檢查時發現，受害之印表機韌體皆未進行更新。

(四)TACERT 接收國外 First 組織資訊時，發現國外亦有相關攻擊行為及討論事項且 HP 原廠亦公告相關文件。

(五)由 HP 原廠公告文件可得知受害型號及解決方法。

參考文件為：

「HPSBPI02728 SSRT100692 rev.5 - Certain HP Printers and HP Digital Senders,Remote Firmware Update Enabled by Default」(HP 原廠公告文件網址列於參考資料)

七、攻擊手法推測

(一)攻擊目標：

HP 公告文件列表之機型且該印表機韌體未進行更新。

(二)攻擊手法：

得知該網頁置換事件時網頁已完成置換，且無法取得置換當時之網路流量及印表機想關資訊，故只能從 HP 原廠公告文件及置換之結果進行推測，推測結果如下：

1. 遭置換之印表機所使用之 IP 皆為公開(Public)IP，可於外部直接連線，且前端無相關資安設備或未進行控管。

2. 該組織或人員先下載原廠印表機韌體，經修改後，再利用 HP 印表機之系統安全漏洞，透過 Port 9100 遠端派送未經授權之印表機韌體進行安裝，以達到網頁置換之目的。

八、應變措施：

(一)更新印表機韌體

由 HP 原廠公告文件得知要修補該系統安全漏洞需進行印表機韌體更新作業，各型號之修正建議請參考 HP 原廠公告文件。

(HP 原廠公告文件網址列於參考資料)

(二)印表機安全性控管

印表機本身如有相關管理介面，皆應有提供系統安全管理選項。建議設定相關選項，以維護印表機安全管理。

(三)網路端安全性控管

由 HP 原廠公告文件中得知，該系統安全漏洞是透過 Port 9100 從遠端派送未經授權之印表機韌體進行安裝。故印表機網路架構前端如有相關資安設備，可利用此規則進行安全管理。

九、參考資料：

(一) HPSBPI02728 SSRT100692 rev.5 - Certain HP Printers and HP Digital Senders, Remote Firmware Update Enabled by Default
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03102449