資訊安全面面觀
從北區A-SOC維運看資訊安全

Outline
大 綱

1 中心簡介

2 營運成果

3 資安
能量整合

4 核心價值

Outline
大 綱

1. 中心簡介
2. 營運成果
3. 資安
   能量整合
4. 核心價值

北區學術資訊安全維運中心（A-SOC）

- 本國**資安資訊分享與分析機制**由行政院**資通安全會報**統籌。教育部配合資安會報建置資安資訊分享與分析中心(A-ISAC)
- 教育部委託本校計資中心成立7×24營運之北區**學術資訊安全維運中心(A-SOC)**，建立**教育體系之資安防護及分析**機制，與**A-ISAC交換資安資訊**

北區A-SOC:營運內容

偵測 分析 通報 諮詢

監看管理範圍：七大區網中心

資安事件偵測：防護學校占全台學校數68%

資安事件偵測量：2020年01月～2020年12月 共計

依標準作業程序執行：程序書19份,管理表單32份

情資偵測與分析

01 TALOS

使用Cisco TALOS 情資，包含：IP、domain、URL、挖礦、釣魚、惡意bot等黑名單，每天即時更新。

02 SNORT

使用商業版Snort rule，目前共有五萬餘條規則，並即時更新動態調整規則，常態開啟之規則約有1萬餘條。

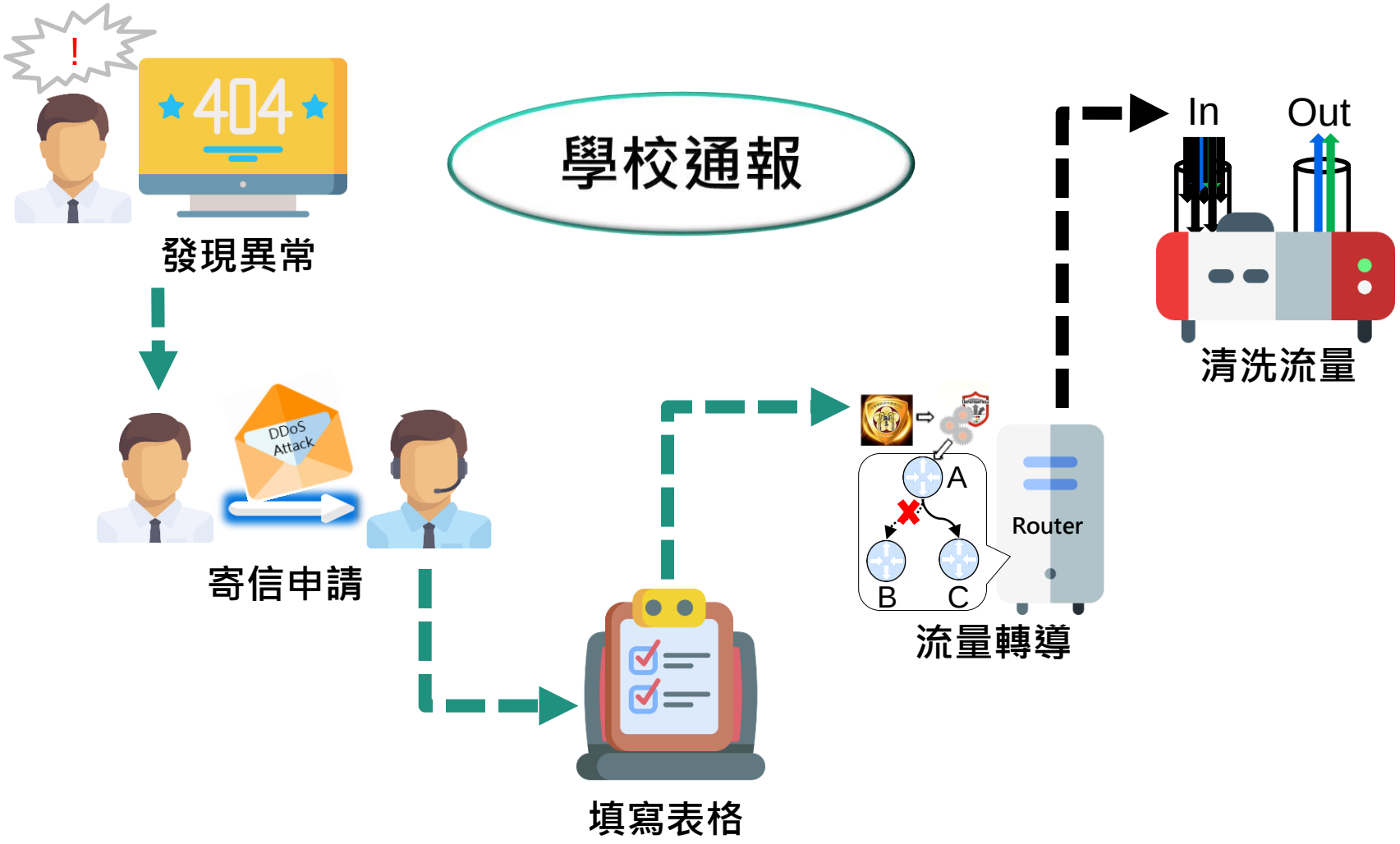
03 ArcSight & ELK

使用 ArcSight 情資整合平台，撰寫事件關聯規則，以及自動化流程；使用ELK視覺化資料庫，進行事件分析，以及大數據應用。

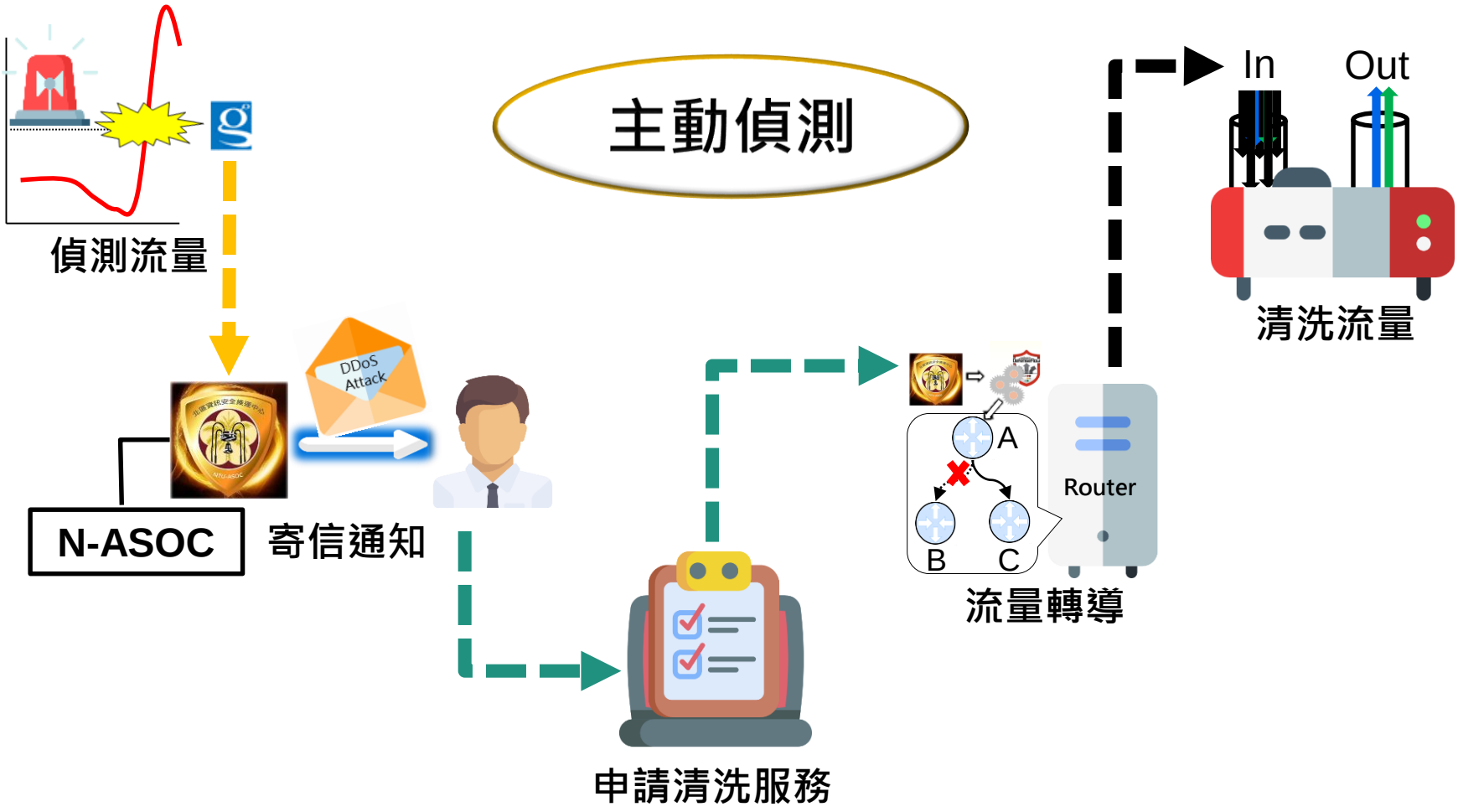
100K
Snort rules intrusion events
Per day

17000K
Security intelligence events

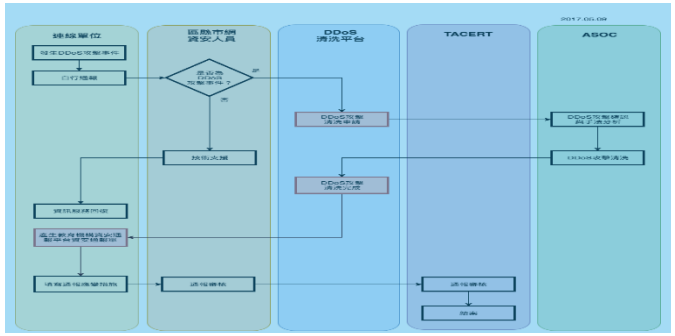
DDoS攻擊偵測與通報架構



DDoS攻擊偵測與通報架構

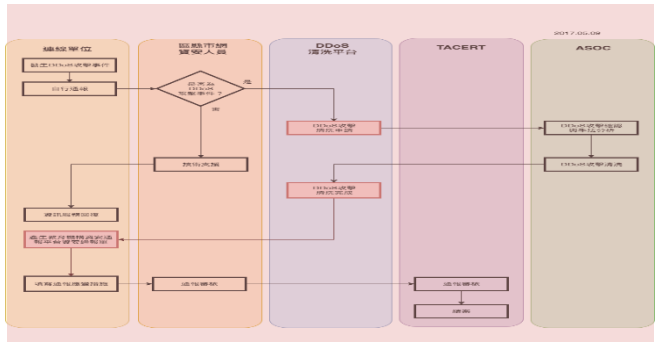


TANet DDoS攻擊防禦作業規定



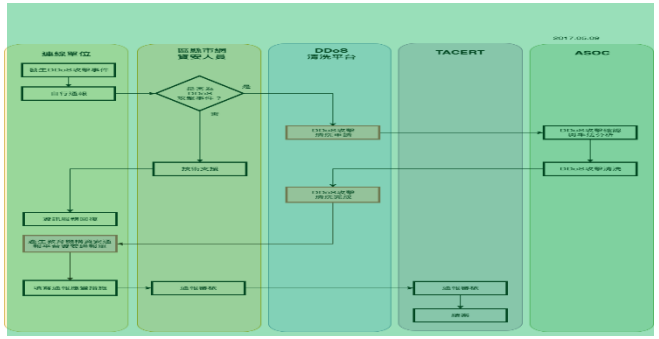
A-SOC主動偵測之通報與防禦

- 北區ASOC骨幹偵測DDoS攻擊後，與下轄單位確認後，執行攻擊流量清洗



單位自行通報之通報與防禦

- 單位自行發現DDoS攻擊， 通報區縣市網，確認後至**TACert**「資安通報系統」申請清洗作業



教育體系單位攻擊其他單位

- 外部單位透過TACERT，通知北區ASOC DDoS攻擊事件，並偕同區縣市網進行清洗作業

TANet DDoS事件通報與應變作業程序

- **學術資訊安全維運中心(南、北A-SOC)**
  - 偵測到大規模DDoS攻擊後，分析DDoS攻擊流量及手法，**發出資安警訊告知連線單位**
  - **接獲TACERT「DDoS通報」申請**或在教育部緊急通知時， 提供DDoS攻擊流量清洗服務，並掌握重大DDoS攻擊事件細節。必要時，A-SOC可**聯繫其他電信業者進行協同作業**

Outline
大 綱

1 中心簡介

2 營運成果

3 資安
能量整合

4 核心價值

DDoS營運成果

漏洞與案例分析

Exchange Server

漏洞說明

CVE-2021-26855是利用Server端偽造SSRF漏洞來進行攻擊

CVE-2021-26857是Unified Messaging服務的反序列化漏洞

CVE-2021-26858及CVE-2021-27065為檔案寫入漏洞，通過身分驗證後可以寫入程式

出處:北區ASOC整理

漏洞攻擊流程

攻擊者從外部經由傳輸埠443連線Exchange Server，並透過CVE-2021-26855 繞過身分驗證進入伺服器，透過CVE-2021-26857 Unified Messaging服務的反序列化漏洞，以該服務的System權限執行任意程式，最後以CVE-2021-26858和CVE-2021-27065任意檔案寫入漏洞，在驗證進入後於Exchange寫入需執行的程式。

資訊安全公司 Huntress 研究人員檢查的超過2000臺Exchange伺服器中，有200臺伺服器已經在其檔案目錄（C:\inetpub\wwwroot\aspnet_client\system_web）中發現web shell程式。

出處:北區ASOC整理

EDR端點防護失效

研究人員指出遭植入web shell的設備皆安裝有（endpoint detection and response, EDR）產品，卻未阻擋web shell的執行，顯示這些攻擊者似乎有方法迴避部分安全產品的偵測。

影響範圍

已知受影響的產品有、2016以及2019Exchange Server2013
微軟表示Exchange 2010不受影響，但基於安全考量也發佈相關安全更新。Exchange Online沒有受到任何影響。

出處:北區ASOC整理

建議處理措施

微軟已在3月2號緊急發佈相關安全公告修補這四項漏洞，同時修補與此次攻擊無關的另外三項漏洞 (CVE-2021-26412、CVE-2021-26854及CVE-2021-27078)，建議用戶盡速更新

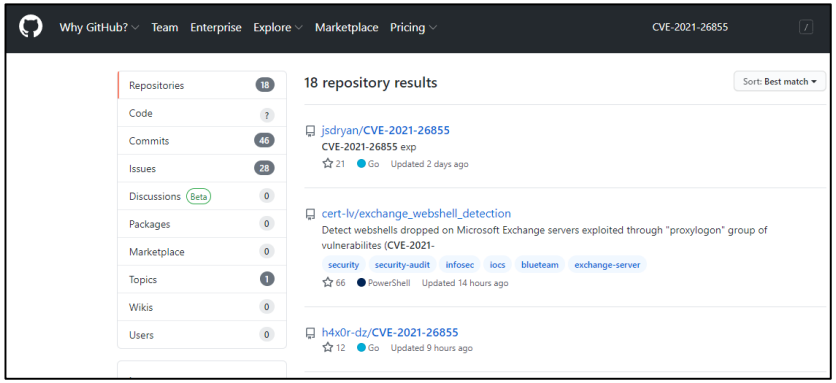
公告連結：https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

建議除立即更新Exchange Server外，也應盡速尋找系統內是否已遭植入web shell，針對此漏洞的研究人員指出，大多數的資安產品皆無法有效防堵透過此漏洞執行的web shell下載

出處:北區ASOC整理

PoC測試-簡介

- 今年三月上旬，在Github已經出現數個針對Exchange Server 漏洞的PoC程式碼，包含對外掃描與自行檢測的版本
- 其中檢查CVE-2021-26855的PoC程式出現最多次
- Github網址：https://github.com/search?q=CVE-2021-26855



Github已經出現數種PoC程式供人下載測試

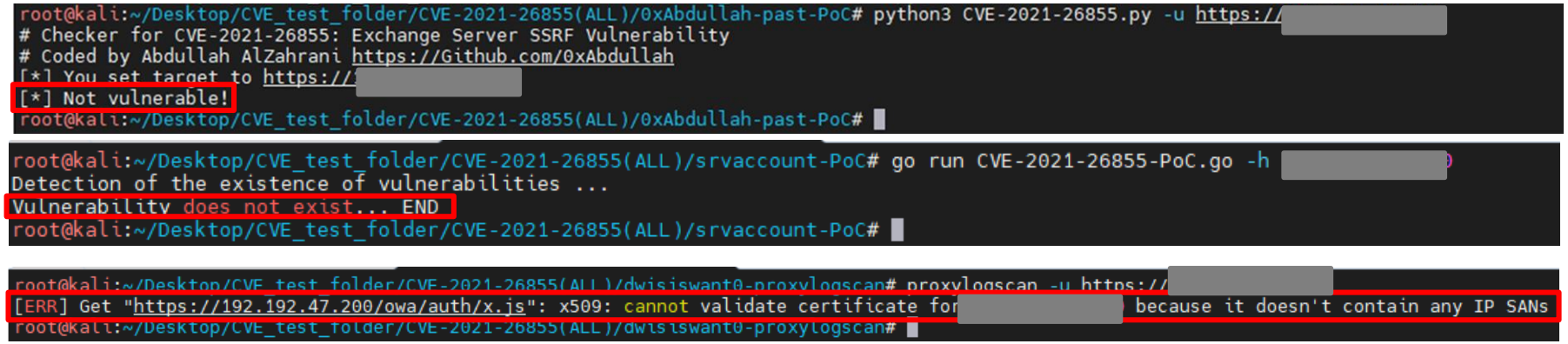
統計日期:2021/03/10	筆數
CVE-2021-26855	18
CVE-2021-26857	5
CVE-2021-26858	5
CVE-2021-27065	6

出處:北區ASOC整理

複測過程截圖記錄

本次範例為複測某機關的紀錄

- 第一張圖片是之前驗證的PoC程式，檢查回傳封包是否帶有特定的字串來判斷是否有漏洞，會直接顯示檢測結果
- 第二張圖片是使用go語言開發的PoC程式，判斷漏洞方式與上方PoC程式相似，也會直接顯示檢測結果
- 第三張圖片是檢測工具包的PoC程式。判斷結果如果是[VLN]為漏洞存在；顯示[ERR]代表漏洞不存在並說明原因



資料來源

1. https://www.ithome.com.tw/news/143001
2. https://www.ithome.com.tw/news/143056
3. https://thehackernews.com/2021/03/urgent-4-actively-exploited-0-day-flaws.html
4. https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
5. https://proxylogon.com/
6. https://github.com/search?q=CVE-2021-26855
7. https://github.com/0xAbdullah/CVE-2021-26855

出處:北區ASOC整理

影印事務機FTP匿名登入問題

事件分析

本次事件問題出自學術單位相當常用影印事務機品牌，KONICA MINOLTA 及其配套軟體 簡易型FTP Server ，“FTPUtility” 該工具程式其它廠牌的事務機一樣可以連線使用，故在業界中是針對事務機掃描檔案分享非常普遍的解決方案

出處:北區ASOC整理

影響範圍

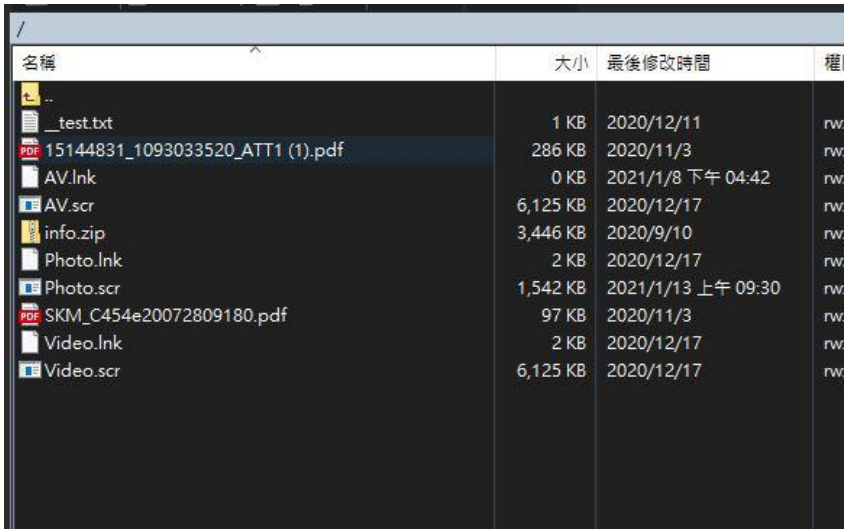
1月底 Shodan 掃描TANet 匿名登入功能開啟設備。於3月初再度掃描，開啟匿名登入裝置有明顯下降

匿名登陸存取

可透過FTP 客戶端程式透過匿名登入，輕易地連線至事務機的檔案共享空間，存取內部掃描文件，有相當大的資料外洩風險。

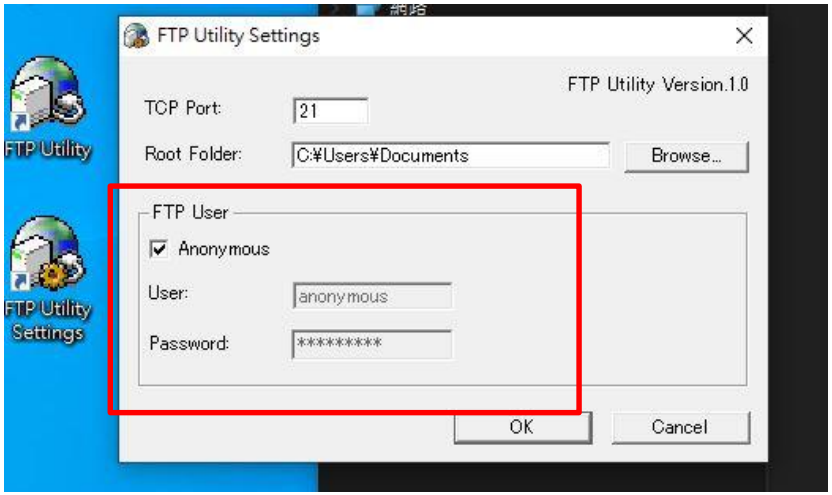
相關攻擊痕跡

已發現多個FTP Server 遭上傳惡意程式包含.scr 執行檔，防毒軟體可判斷出為惡意的挖礦程式。



建議防護措施

建議於事務機的共享FTP SERVER 設定帳號密碼及權限管控以免造成文件外洩與成為駭客上傳檔案的管道。



F5 BIG-IP BIG-IQ 漏洞說明

漏洞概述

- F5 Networks 于3月10日發布的漏洞公告中包含 BIG-IP與BIG-IQ 產品的七項漏洞。

- 其中CVE-2021-22986、CVE-2021-22987、CVE-2021-22991、CVE-2021-22992屬於重大漏洞，CVSS 風險評分皆超過9.0分，CVE-2021-22986 更可繞過身分驗證遠端行任意命令。

出處:北區ASOC整理

漏洞說明

- CVE-2021-22986　iControl REST界面中的未經身份驗證遠程命令執行漏洞。
- CVE-2021-22987　TMUI驗證的遠程命令執行漏洞
- CVE-2021-22991　TMM 緩衝區溢出漏洞
- CVE-2021-22992　WAF/ASM緩衝區溢出漏洞

出處:北區ASOC整理

CVE-2021-22986 攻擊流程

CVE-2021-22986 為未經身份驗證遠程命令執行漏洞。該漏洞的CVSS評分為9.8，並同時影響到BIG-IP和BIG-IQ。

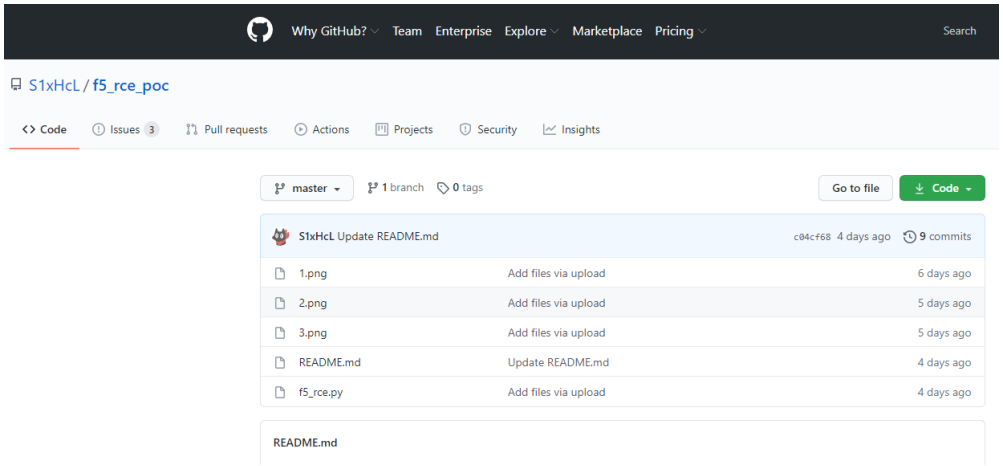
未經身分驗證的攻擊者只要能夠透過外部網路存取到iControl REST 管理介面，即可利用路徑/mgmt/tm/util/bash 作為攻擊的進入點，發送HTTP POST夾帶特定的JSON 欄位command及CmdArgs即可成功執行任意指令。

出處:北區ASOC整理

CVE-2021-22986 POC-1

近期在Github已經出現數個PoC程式碼。

Github網址：
https://github.com/S1xHcL/f5_rce_poc/blob/master/f5_rce.py



出處:北區ASOC整理

CVE-2021-22986 POC-2

Shodan 搜尋F5關鍵字

經篩選後學術網路曝險設備總數為22台

出處:北區ASOC整理

CVE-2021-22986 POC-3

- 3月22日POC測試結果，可成功執行id 指令設備為1台：

- 經通報後於3月25日進行二次掃描，已確認曝險設備修補完成。

出處:北區ASOC整理

影響範圍

受影響的產品如下：

- BIG IP
  - 16.0.1.1
  - 15.1.2.1
  - 14.1.4
  - 13.1.3.6
  - 12.1.5.3
  - 11.6.5.3
- BIG IQ
  - 8.0.0
  - 7.1.0.3
  - 7.0.0.2

出處:北區ASOC整理

建議處理措施

F5已在3月10號發佈相關安全公告修補，建議用戶盡速更新。

公告連結：
https://support.f5.com/csp/article/K02566623

出處:北區ASOC整理

參考連結

1. https://support.f5.com/csp/article/K02566623
2. https://www.nccst.nat.gov.tw/VulnerabilityDetail?seq=1147
3. https://securityaffairs.co/wordpress/115760/hacking/f5-big-ip-attacks-cve-2021-22986.html
4. https://github.com/S1xHcL/f5_rce_poc
5. https://www.ithome.com.tw/news/143171

出處:北區ASOC整理

Outline
大 綱

1 中心簡介

2 營運成果

3 資安
能量整合

4 核心價值

Outline
大 綱

1 中心簡介

2 營運成果

3 資安
能量整合

4 核心價值

ASOC核心價值


建置符合教育體系特色之資安防護
遵循行政院國家資通安全通報應變流程
架構七大區網
中心資安防護網
提供全年無休
資安偵測與監看
依據標準
作業程序作業
達到即時快速
資安防禦與管理
持續精進最新
資安攻防技術

加密貨幣劫持說明與防護措施建議

加密貨幣劫持

- 挖礦劫持是近年來相當盛行的一種惡意行為，攻擊者會利用受感染裝置的處理能力與網路頻寬來賺取加密貨幣。
- 負責此類活動的惡意挖礦程式用意在於盜取資源，並且能夠長時間且不被注意到的裝置如 NAS 、DVR監控主機等等往往也會成為重點目標。
- 加密貨幣的挖掘需要大量的處理運算能力，故惡意挖礦程式網網具備快速的內網擴散能力，進而蒐集到足夠的算力執行挖礦活動營利。

惡意挖礦程式的感染方式

加密貨幣挖掘程式的感染途徑主要分為以下三種：

1. 免費共享軟體夾帶
2. 漏洞攻擊
3. 網頁端植入惡意腳本

加密貨幣劫持常用工具XMRig

```
 * ABOUT        XMRig/2.14.1 clang/10.0.0
 * LIBS         libuv/1.27.0 OpenSSL/1.0.2r microhttpd/0.9.62
 * CPU          Intel(R) Core(TM) i7-4770HQ CPU @ 2.20GHz (1) x64 AES AVX2
 * CPU L2/L3    1.0 MB/6.0 MB
 * THREADS      3, cryptonight, av=0, donate=5%
 * ASSEMBLY     auto:intel
 * POOL #1      pool.hashvault.pro:3333 variant auto
 * COMMANDS     hashrate, pause, resume
[2019-04-01 12:07:26] use pool pool.hashvault.pro:3333  193.70.102.216
[2019-04-01 12:07:26] new job from pool.hashvault.pro:3333 diff 5000 algo cn/r height 1803431
[2019-04-01 12:07:27] READY (CPU) threads 3(3) huge pages 0/3 0% memory 6144 KB
[2019-04-01 12:07:48] accepted (1/0) diff 5000 (200 ms)
[2019-04-01 12:08:22] accepted (2/0) diff 5000 (73 ms)
[2019-04-01 12:08:28] speed 10s/60s/15m 84.8 98.0 n/a H/s max 101.8 H/s
[2019-04-01 12:09:20] new job from pool.hashvault.pro:3333 diff 5000 algo cn/r height 1803432
[2019-04-01 12:09:28] speed 10s/60s/15m 100.9 101.0 n/a H/s max 102.0 H/s
```

XMRig程式執行畫面

如何防護加密貨幣劫持

根據賽門鐵克網路安全威脅報告，於2017年加密貨幣劫持攻擊事件數量爆漲8500%，顯示加密貨幣的價值增長，導致網路攻擊者試圖從加密貨幣的市場中獲利。

若想從這波加密貨幣劫持的浪潮中全身而退，使用者可參照以下防護準則：

1. 養成良好的網路使用習慣

2. 請勿從非官方網站中下載共享軟體，並確實檢查安裝過程中是否要求安裝多餘的程式。

3. 提升對電子郵件社交工程攻擊的防護意識

4. 安裝正版防毒軟體並自動更新病毒碼及定期進行系統弱點掃描

5. 建立NAT log 機制，便於快速鎖定發生資安事件之主機

印表機 FTP 匿名登入問題

北區ASOC團隊

資料更新日期：2021/04/14

前言

- 現在的網路印表機已經從單純的印表機變成多功能事務機(Multi-Function Printer)，包含印表機、掃描器、傳真機、影印機等功能。有些印表機還有安裝Wi-Fi網卡，支援Google Cloud Print 和Apple AirPrint等雲端列印服務。
- 目前整理出幾個有關印表機FTP的問題，並且在某些問題適度地提供建議方式。

- 備註：後續投影片把「多功能事務機」都稱為「印表機」。

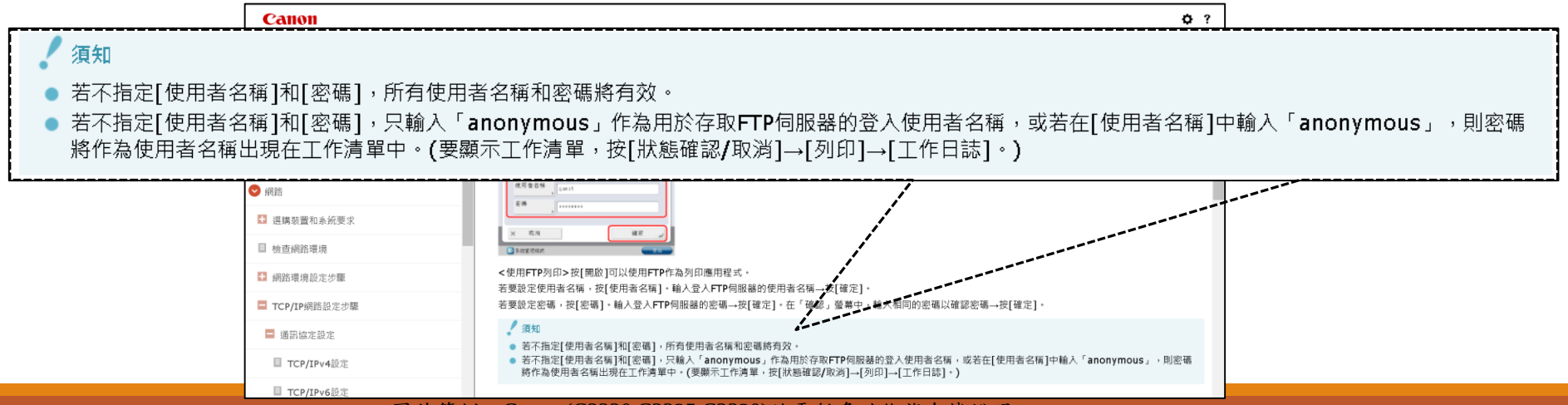
問題整理

- Q1. 是否所有印表機都有預先開啟FTP匿名登入？
- Q2. 是否所有印表機都有硬碟？
- Q3. 印表機內部記憶體是否會長時間紀錄資料？
- Q4. 印表機廠牌提供程式是否有FTP功能？
- Q5. 如果印表機改為虛擬IP，要如何讓特定使用者連上使用？

Q1.是否所有印表機都有預先開啟FTP匿名登入？

- 經詢問相關人士，如果廠牌為HP或Konica Minolta，低規格(小型)的機體不具備FTP功能，但中高規格以上基本都會有FTP功能。

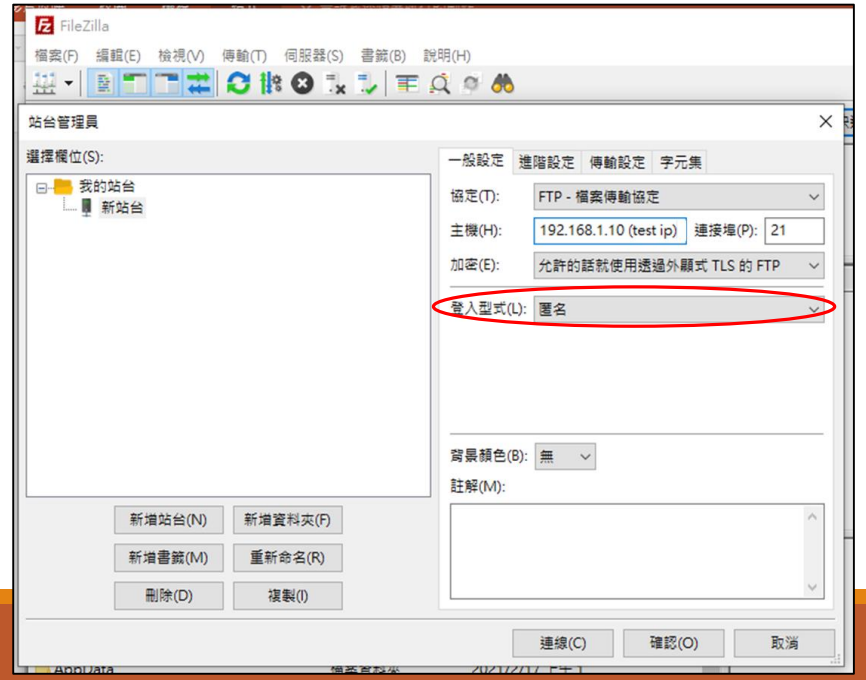
- 從網路上查詢各家印表機的說明手冊後，經整理後的相關資訊如下：
  1. **Ricoh**：初始在設定FTP時就會要求設定帳號密碼，有提供軟體進行FTP設定
  2. **HP**：初始要求設定帳號密碼，可匿名登入，有提供軟體進行FTP設定
  3. **Canon**： FTP預設匿名登入，有提供軟體進行FTP設定
  4. **Konica Minolta**：有提供軟體進行FTP設定，軟體本身預設匿名登入。

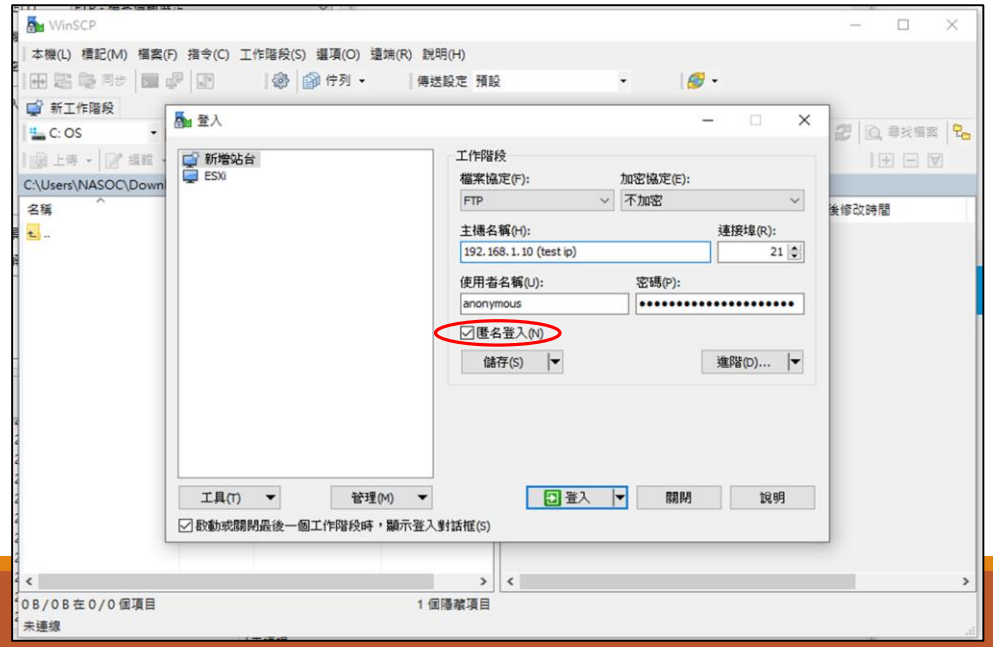


圖片範例：Canon (C3330 C3325 C3320)的雷射多功能複合機說明
資料來源：https://oip.manual.canon/USRMA-0319-zz-CS-zhTW/frame_htmls/home.html

Q1.是否所有印表機都有預先開啟FTP匿名登入？

- 建議管理印表機的人員登入設備檢查，或是利用相關FTP工具進行測試
- 常用的FTP工具(下載安裝後，請選擇匿名登入，輸入印表機IP位置後測試)：
  1. 左圖：FileZilla (官方網站： https://filezilla-project.org/)
  2. 右圖：WinSCP (官方網站： https://winscp.net/eng/index.php)





Q2.是否所有印表機都有硬碟？

- 以Konica Minolta廠牌來說，小型的印表機只使用設備本身的記憶體，而落地型的印表機(事務機、複合機之類)較有機會視需求去擴充。
- 通常各廠牌的小型印表機在設計之初就無設計額外安裝硬碟的空間。

Q2.是否所有印表機都有硬碟？

- 通常印表機廠商都會寫上該設備的規格，找記憶體相關的說明就可以得知此型號的印表機是否可以安裝硬碟。
- 可參考下圖範例

資料來源：https://www.aurora.com.tw/oa/product/0h069340399482009359

Q3.印表機內部記憶體是否會長時間紀錄資料？

- 大多數印表機的預設設定是在列印完成後，會刪除記憶體內的資料。
- 如果發生資料傳輸中斷或沒有列印完成，有可能會讓資料暫時儲存在記憶體內，直到列印任務完成為止。
- 部分印表機廠牌機型有提供列印文件的儲存時間設定，如果待列印文件儲存於記憶體超過一定時間，會自動自行刪除檔案。

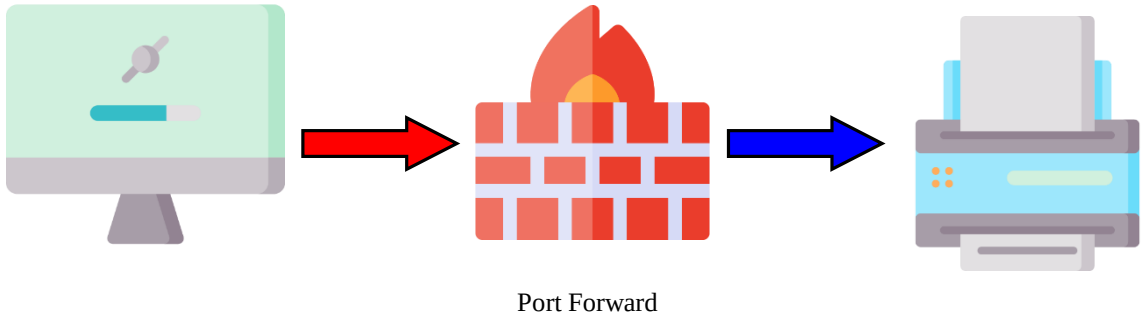
Q4.印表機廠牌提供程式是否有FTP功能？

- 大部分印表機原廠提供的管理程式，都可以設定FTP相關功能
- 並非每一家廠商的管理程式會要求使用者建立一組登入使用的帳號密碼
- 網路上有些公司(非原廠軟體)會提供簡易FTP軟體可以讓使用者輕鬆架設FTP Server，如果使用者設定不當也可能會開啟FTP匿名登入。
- 下面列表為可架設FTP Server軟體：
  1. Quick'n Easy FTP Server Lite
  2. FTP Utility
  3. KM FTP
  4. PCMAN FTP Server

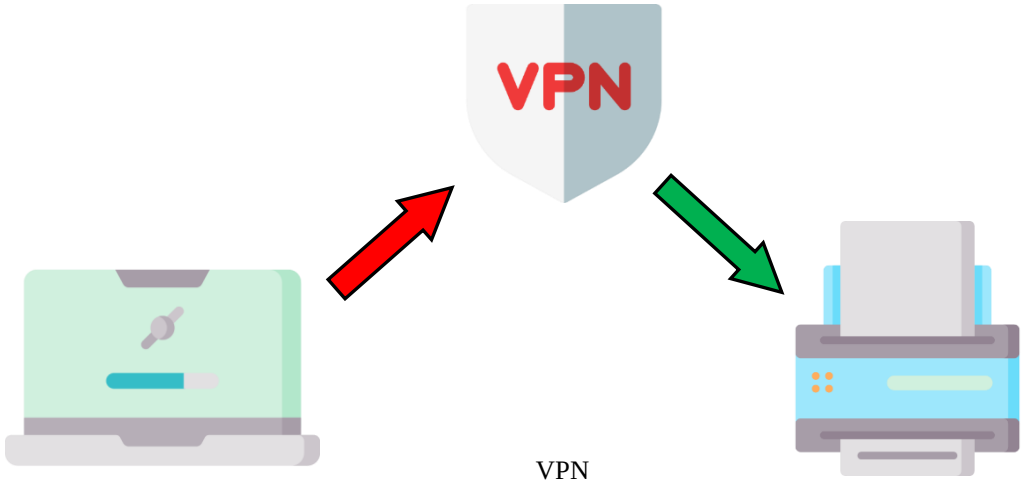
- 備註：
  - 參考網址1： https://keyu.com.tw/?page_id=459
  - 參考網址2： http://oa-gstar.com.tw/wp/driver-download/

Q5.如果印表機改為虛擬IP，要如何讓特定使用者連上使用？

- 有兩個方式可以達成：
  - A. Port Forward (適合單一、固定IP情況使用)
  - B. VPN (適合多個、不固定IP情況使用)



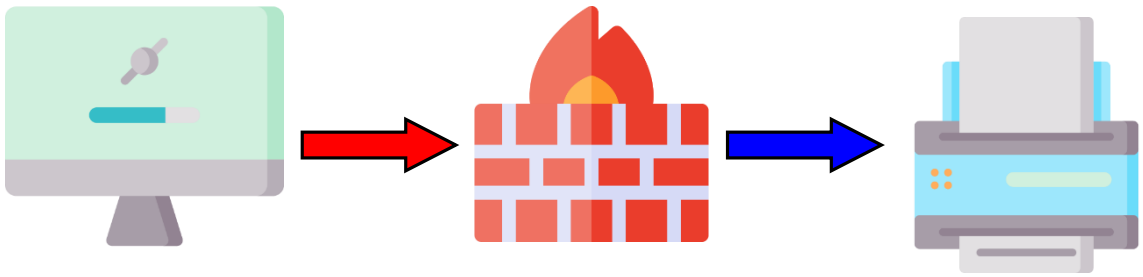
Port Forward



VPN

Q5.如果印表機改為虛擬IP，要如何讓特定使用者連上使用？

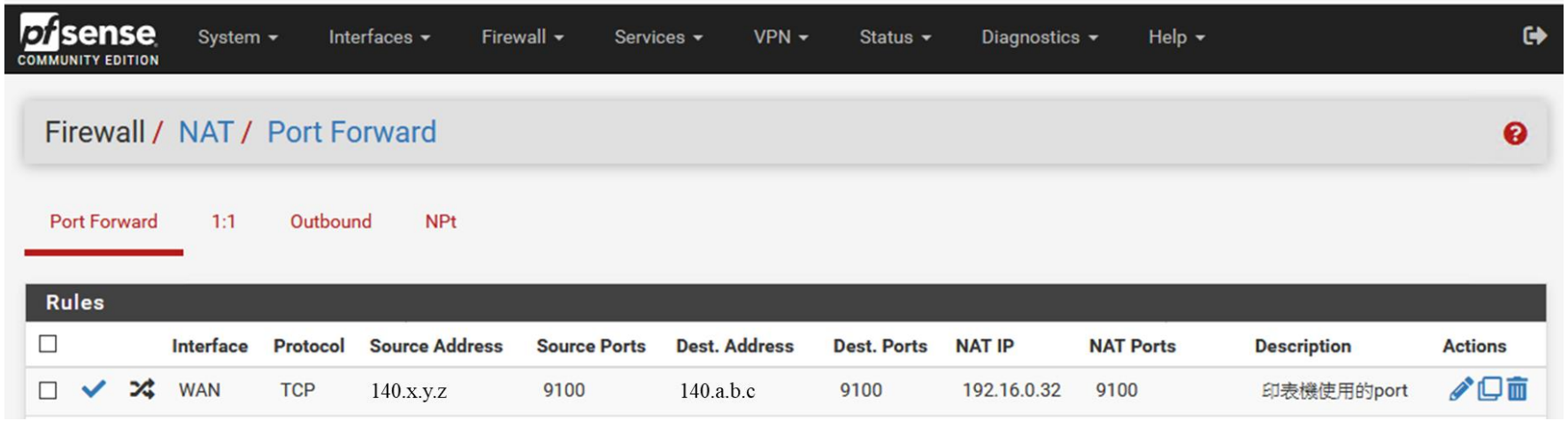
- Port Forward方式：
  - 首先，當印表機接在某些網路設備(例如：防火牆、無線路由器、交換器...等)之後，請先檢查此印表機是否有被分配到虛擬IP，之後確認要連入的固定IP
  - 確定印表機的IP為虛擬IP後，登入分派虛擬IP的網路設備，調整連線的規則
  - 規則設定的原則：讓WAN端的IP在指定範圍的Port，連到LAN端的印表機的連接的Port



Port Forward

Q5.如果印表機改為虛擬IP，要如何讓特定使用者連上使用？

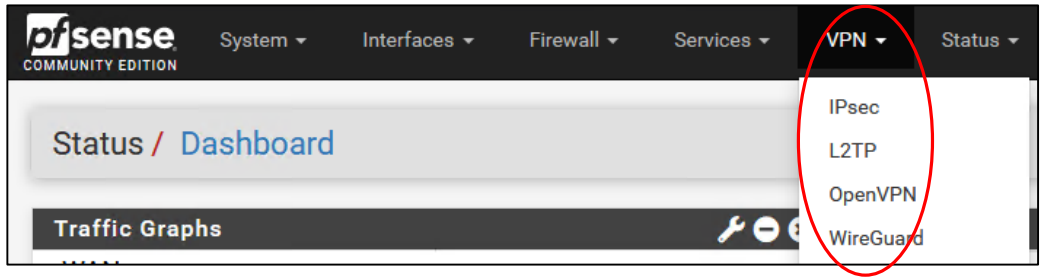
- Port Forward範例情境：某學校教授想在自己的辦公室(IP：140.x.y.z)使用放在實驗室(IP：140.a.b.c)的印表機，但因辦公室和實驗室是不同IP網段，而且印表機接在防火牆後面並使用虛擬IP(IP：192.168.0.32)。
  - 網管人員需要在防火牆上幫教授設定Port Forward，讓教授能順利連上印表機。
  - 此時Source IP為140.x.y.z；Destination IP為140.a.b.c ； Port Forward後的IP為192.168.0.32 ；而印表機使用的port為9100，所以設定方式可參考下圖範例：



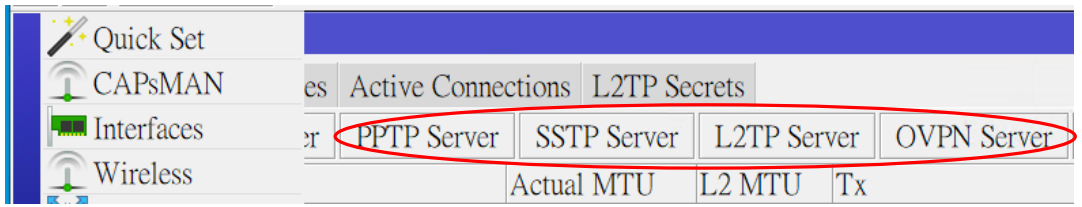
在pfsense上設定Port Forward

Q5.如果印表機改為虛擬IP，要如何讓特定使用者連上使用？

- VPN方式：
  - 首先，當印表機接在某些網路設備(例如：防火牆、無線路由器、交換器...等)之後，請先檢查此印表機是否有被分配到虛擬IP。
  - 某些網路設備有內建VPN服務，請查詢該設備的說明手冊建立。
  - 當要使用VPN服務時，請使用對應的VPN服務方式連線。成功連上VPN後，再連線至印表機的虛擬IP使用列印服務。



pfsense內建的VPN服務



RouterOS內建的VPN服務

資料來源

1. Day 23 等著被駭的多功能事務機 Multi-Function Printer：https://ithelp.ithome.com.tw/articles/10196804
2. 印表機資料-1：https://www.aurora.com.tw/oa/product/0h069340399482009359
3. 印表機資料-2：https://www.brother.tw/-/media/ap/Taiwan/Products/Common/Brochures/HL-L2320D/DLL_2020.pdf
4. 印表機資料-3：https://oip.manual.canon/USRMA-0319-zz-CS-zhTW/frame_htmls/home.html
5. FTP軟體提供參考網址-1： https://keyu.com.tw/?page_id=459
6. FTP軟體提供參考參考網址-2： http://oa-gstar.com.tw/wp/driver-download/

圖片來源

- 本次簡報內的icon圖片：https://www.flaticon.com/ (作者：Freepik)

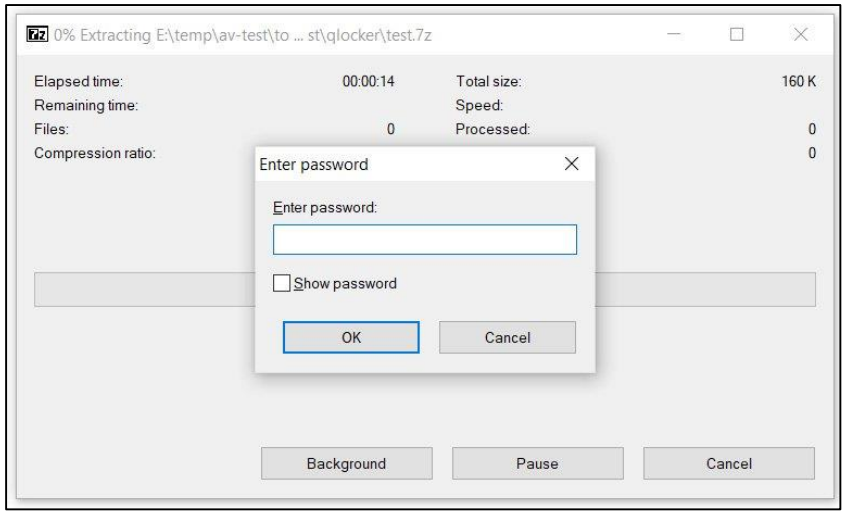
近期QNAP重大漏洞說明

北區ASOC團隊

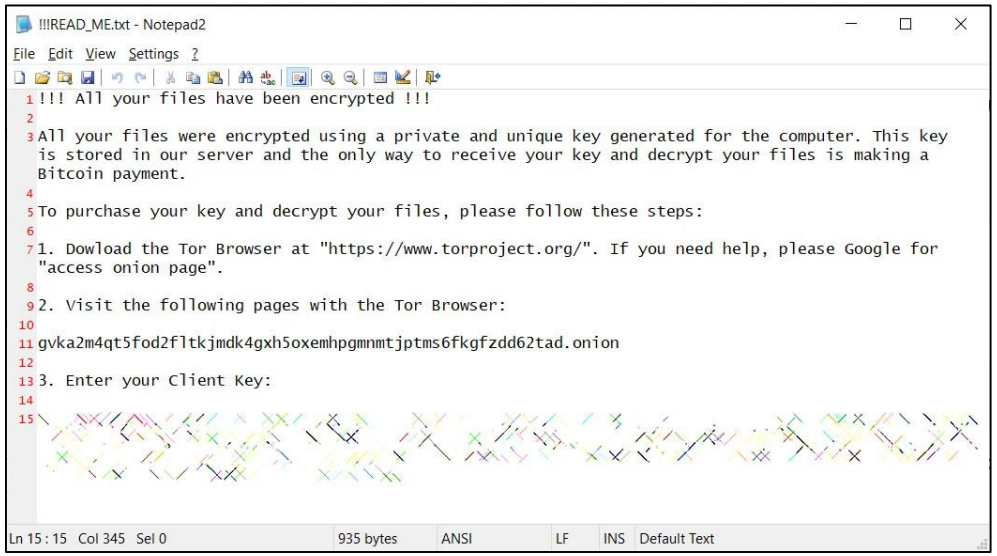
資料更新日期：2021/04/29

事件說明

- 自4月19日起QNAP(威聯通)品牌 NAS 陸續傳出遭駭客鎖定發動攻擊，並透過名為Qlocker的勒索軟體將檔案加密，把檔案加密變成.7z，且留下勒索訊息要求受害者支付0.01個比特幣。
- 本次漏洞在2020年11月便被資安公司SAM Seamless Network發現並通報QNAP。由於該漏洞能夠繞過身分驗證，透過本次漏洞可以讓惡意人士於遠端方式以root權限執行任意命令。



檔案被加密後，需要輸入密碼才能解開檔案

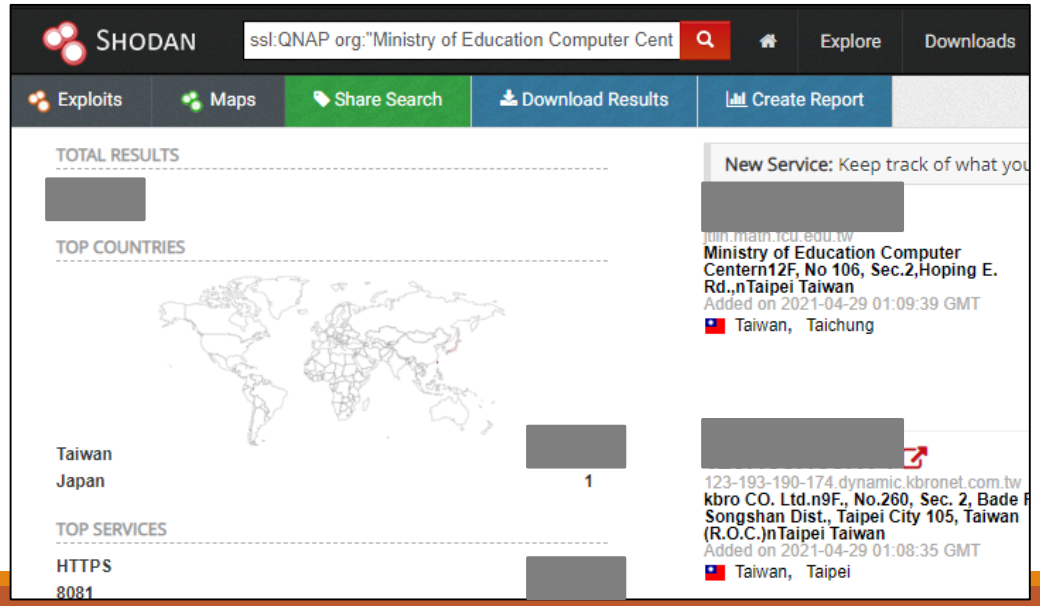


Qlocker勒索軟體所產生的勒索訊息

上述圖片的資料來源：https://www.bleepingcomputer.com/news/security/massive-qlocker-ransomware-attack-uses-7zip-to-encrypt-qnap-devices/

學網內部的QNAP設備數量

- 目前透過Shodan搜尋TANet內部的QNAP設備，總數量為[redacted]筆
- 北區ASOC實際下載到的Shodan資料數量是[redacted]筆，扣除重複的IP資料和非學術網路的IP資料後剩下[redacted]筆。



影響範圍

- 受影響之QNAP設備如下：
  1. CVE-2020-2509：
     - ✓ 所有QNAP設備
  2. CVE-2020-36195：
     - ✓ 啟用Multimedia Console與Media Streaming Add-on應用程式之QNAP設備
  3. CVE-2021-28798：
     - ✓ TS-112P、TAS-168、TAS-268之QTS 4.3.3.1624 build 20210416以前版本
  4. CVE-2021-28799：
     - ✓ 啟用HBS 3 Hybrid Backup Sync應用程式之QNAP設備

無效的防護措施

- 由於此漏洞能夠繞過身分驗證，以下防護措施是無效的：
  1. 停用admin 帳密
     - 該漏洞無須透過帳號密碼登入即可成功執行命令
  2. 修改預設port
     - 透過自動port scan工具可輕易找出對應的port號
  3. 開啟密碼暴力破解防護，多次密碼錯誤封鎖IP
     - 同上該漏洞無須透過密碼登入，故不會有嘗試登入之行為
  4. 透過防火牆阻擋
     - L3/L4防火牆無法阻擋此次攻擊，需透過L7 防火牆或WAF並且須即時更新偵測規則才可供阻擋攻擊

建議防護措施

1. 更新QTS作業系統版本
   - 目前QNAP官方已針對此漏洞釋出更新程式，請盡速更新至修補此漏洞的版本。
2. 請勿將NAS透過Public IP 連線網路
   - 一旦NAS暴露於公開網路，當發生重大漏洞時往往將成為被攻擊的首要目標
3. 透過VPN 連線遠端NAS設備

參考資料

1. 雷神講堂：https://www.facebook.com/groups/rayforum/permalink/3902801303133332
2. iThome 論壇：https://www.ithome.com.tw/news/144004
3. SAM Seamless Network：https://securingsam.com/new-vulnerabilities-allow-complete-takeover/
4. BleepingComupter：https://www.bleepingcomputer.com/news/security/massive-qlocker-ransomware-attack-uses-7zip-to-encrypt-qnap-devices/