資訊安全面面觀

臺灣大學計算機及資訊網路中心
李美雯

DDoS事件通報與應變作業程序

- **分級措施**
  - **連線單位**
    - **疑似遭受DDoS攻擊，通報所屬區、縣(市)網路中心**協助確認或技術支援。確認申請清洗服務時請區、縣(市)網路中心至**TACERT提出申請**
    - **清洗結束後**，參考『教育機構資安通報應變手冊』及『國家資通安全通報應變作業綱要』，判定DDoS攻擊之事件等級，**於時限內至TACERT的「教育機構資安通報平台」填寫《資安通報單》**，以完成通報應變作業

TANet DDoS事件通報與應變作業程序

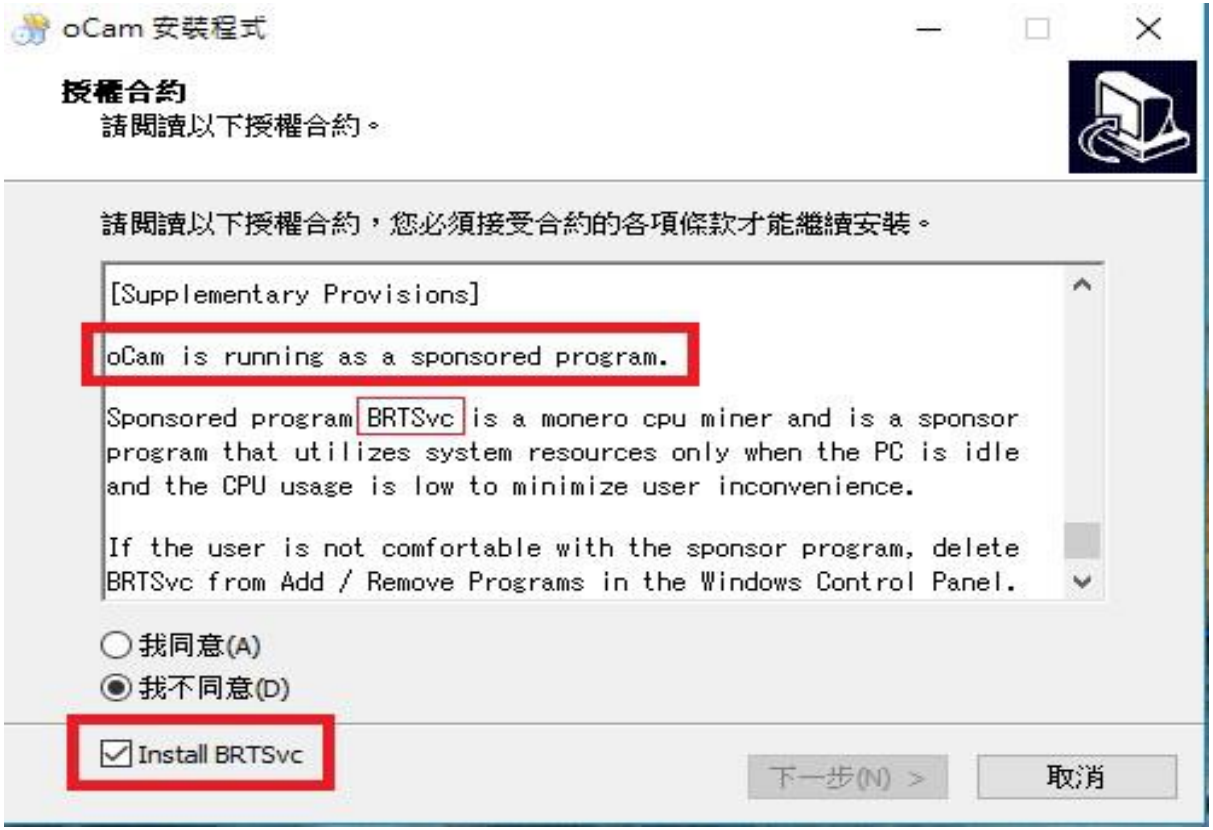
- **區(縣)市網路中心**
  - 確認轄下單位需申請清洗，請至**TACERT「資安通報報表系統」項下「DDoS通報」提出**申請
  - 當DDoS攻擊事件完成清洗後**登入TACERT 「教育機構資安通報平臺」進行資安事件審核**

資安案例分享

ohSoft 軟體挖礦事件

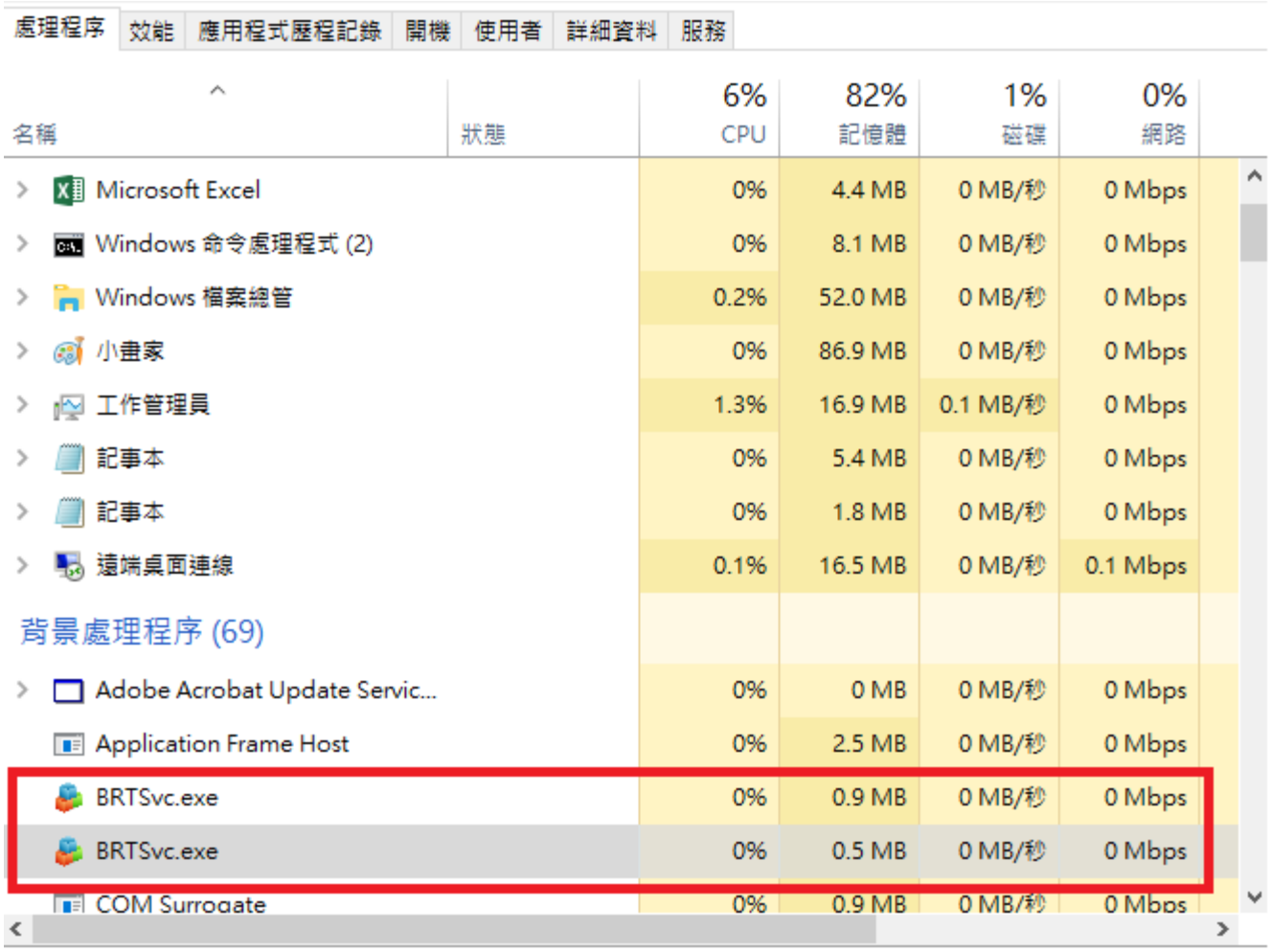
- 學校老師反應免費螢幕錄製軟體oCam夾帶挖礦程式 BRTSvc.exe，進而發現ohsoft旗下所有軟體(oCam、VirtualDVD、Secret Folder等)皆有此情況。

- 如下圖所示，oCam 安裝主程式的合約中，使用者除同意成為挖礦程式的贊助者，並且預設同意安裝挖礦程式BRTSvc.exe 。



ohSoft 軟體挖礦事件

挖礦程式BRTSvc.exe本身不會長時間佔用主機之網路或CUP



ohSoft 軟體挖礦事件

- 挖礦程式BRTSvc不會隨者主程式移除而移除，可利用新增/移除程式移除。
- 移除時建議打開工作管理員關閉相關程式，或是檢查是否被防毒軟體隔離，導致無法移除。

CVE-2020-0796 漏洞簡介

- 3/10微軟修補程式日(Patch Tuesday)的更新修補中，漏修補Server Message Block 3.1.1 (SMBv3)漏洞
- 此漏洞的嚴重程度與永恆之藍(EternalBlue)攻擊程式所利用的CVE-2017-0145一樣危險
- 在Github上已經有數個PoC程式去驗證此漏洞
- 如果此漏洞遭人利用而發動攻擊，極可能會發生跟WannaCry同樣等級的災難

漏洞原因

- 漏洞發生在srv2.sys檔案的 Srv2DecompressData函式
- 由於SMBv3在傳送資料前會壓縮資料，並在記憶體中配置一個解壓縮緩衝區(Buffer)
- 而傳送資料的過程中上述的函式並沒有檢查封包長度，導致攻擊者可設計異常的封包長度，造成緩衝區發生溢位(overflow)

影響版本

- 此漏洞會影響使用SMBv3服務的作業系統：
  - Windows 10 Version 1903/1909
  - Windows Server Version 1903/1909

備註： Windows 7 與 Windows Server 2008 R2 以前的版本，SMBv2, SMBv1不會受到此漏洞影響。但如果沒有使用上的需求，建議關閉SMB相關服務來降低被攻擊的風險。

建議措施

1. 更新微軟的修補漏洞程式(下載網址：https://www.catalog.update.microsoft.com/Search.aspx?q=KB4551762)
2. 在防火牆、路由器等網路設備上設定阻擋或關閉 port 445 的連線
3. 若轄下學校未設置防火牆設備則建議，利用各區網ASR阻擋445port 連線

新冠肺炎釣出網路釣魚攻擊

- **背景說明**
  - 駭客乘新冠肺炎(COVID-19)病毒於全球大肆傳播感染之際，利用聳動標題散播網路釣魚信件
  - APT組織 MustangPanda 透過電子郵件散佈惡意程式
  - 此次社交工程郵件內文包含繁體中文，且以政府官員名義於Facebook對疫情發言，誘使使用者開啟郵件附件

新冠肺炎釣出網路釣魚攻擊

- **攻擊分析**
  - 利用包含HTML程式碼與VBScript標籤 的惡意link 文件
  - 透過Windows 內建可用於執行HTML文件的Mshta.exe於背景執行其惡意的VBScript程式碼

新冠肺炎釣出網路釣魚攻擊

- **建議處理措施**
  - **關閉郵件預覽視窗**，未關閉郵件預覽開啟惡意郵件圖檔會自動執行惡意程式。
  - **關閉郵件自動下載圖片**，未關閉遠端郵件圖片下載，開啟惡意郵件會被追蹤郵件讀取紀錄。
  - **定期更新主機**防毒軟體病毒碼且進行全機掃描
  - **定期更新系統漏洞**
  - **不開啟來路不明的電子郵件**，開啟前請謹慎確認寄件者、主旨與內容

QNAP再度遭受攻擊

- **前言**
  - 今年6月研究人員發現eCh0raix勒索軟體組織針對QNAP NAS 軟體漏洞發動了另一波的勒索病毒攻擊

- **漏洞簡介**
  - eCh0raix利用QNAP NAS 線上相簿程式 Photo Station漏洞，分別是CVE-2019-7193、CVE-2019-7194及CVE-2019-7195
  - 三個重大漏洞的CVSS風險評分皆為9.8，遠端攻擊者可對目標設備發送特製的請求，利用此漏洞進而執行任意程式碼

QNAP再度遭受攻擊

- **受影響之版本與平台**
  - Photo Station 5.2.11
  - Photo Station 5.4.9
  - Photo Station 6.0.3

- **建議處理措施**
  - QNAP官方已針對此漏洞釋出更新程式，請各機關聯絡設備維護廠商進行版本確認並將設備更新至以下版本
    - QTS：
    - QTS 4.4.1：build 20190918(含)以後版本
    - QTS 4.3.6：build 20190919(含)以後版本

QNAP再度遭受攻擊

- Photo Station：
  - QTS 4.4.1：Photo Station 6.0.3(含)以後版本
  - QTS 4.3.4 ~ QTS 4.4.0：Photo Station 5.7.10(含)以後版本
  - QTS 4.3.0 ~ QTS 4.3.3：Photo Station 5.4.9(含)以後版本
  - QTS 4.2.6：Photo Station 5.2.11(含)以後版本

- **安全建議設定**
  - 開啟網路存取防護 /異常連線 IP 自動封鎖，阻擋暴力密碼攻擊
  - 安裝QNAP 官方防毒軟體Malware Remover，並定期掃描裝置

QNAP再度遭受攻擊

- 建立一個具有admin權限的新帳號，使用安全性高的密碼(建議用數字、大小字母、特殊符號混和；密碼長度>8)，之後關閉admin帳號
- 如果沒有使用ssh與telnet服務的需求，請關閉這兩個服務
- 修改預設連接埠(例如：443 或 8080...等)