107 年度北區區網委員會第二次會議(2018.12.25)

一、資安通報宣導

發現資安事件後除應循內部程序上報外，並須於 1 小時內，至通報應變網站通報登錄資安事件細節

二、區網營運業務報告

(1)Routing loop 分析

偵測方法:

Ping:Both

Tracert:Both

Netflow:僅能在各自 Router 上偵測

(2)DDoS 案例分析

DDoS 攻擊方法

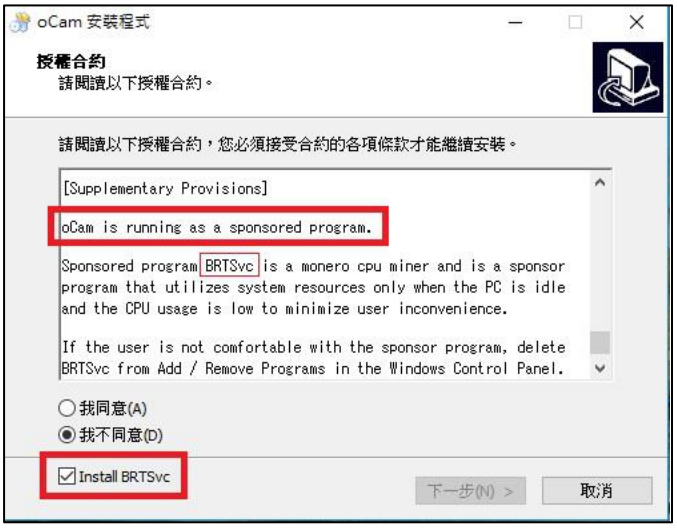
新型 LDAP 攻擊取代傳統 DNS、NTP 放大攻擊

DDoS 攻擊來源

過去使用 Internet Server(NTP, Open Resolver)轉而利用現成雲端資源

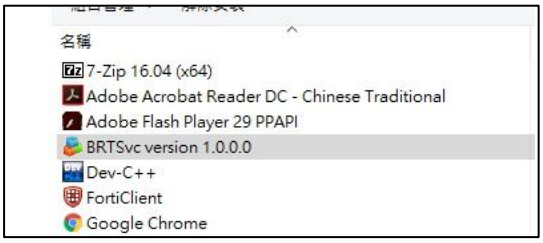
三、挖礦事件(1)

OCAM 含有挖礦程式，經查測 ohsoft 旗下所有軟體(oCam、VirtualDVD、Secret Folder 等)皆有此情況



挖礦程式移除

BRTSvc 須單獨移除，此挖礦程式不會隨者主程式移除而移除，使用新增/移除程式即可順利移除。



四、挖礦事件(2)

BluestacksAndroid 模擬器，安裝程式疑似被植入挖礦。

解決方式：

模擬器版本更新或直接移除

五、台師大網路電話系統建置暨使用經驗分享

傳統交換機問題：

交換機老舊已達淘汰年限

三校區各系所有自己的交換機，無法統一控管

總機系統各自獨立，撥碼方式混亂

導入 VOIP 後的效益

全校話費從原本 90 萬/月，降至 64 萬/月

提升三校區便利性(四碼直播及來電轉接)