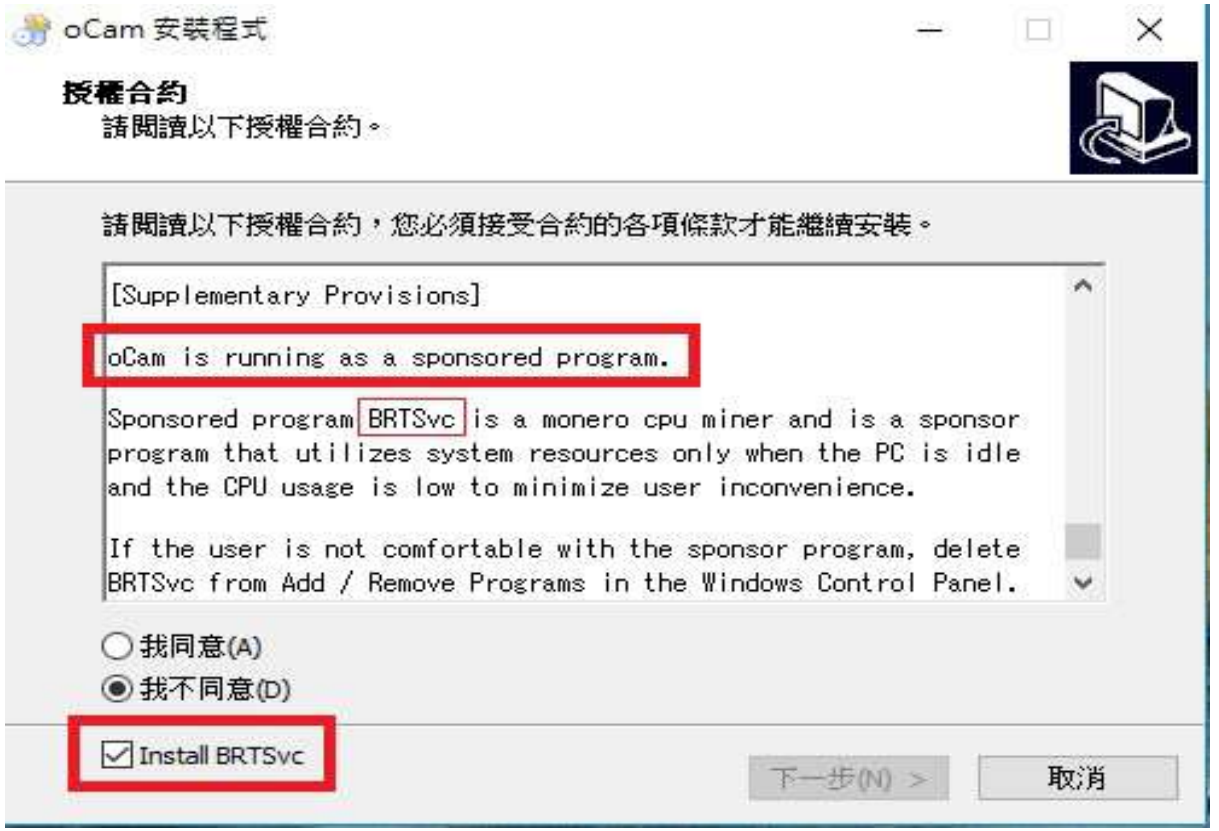
Ocam報告

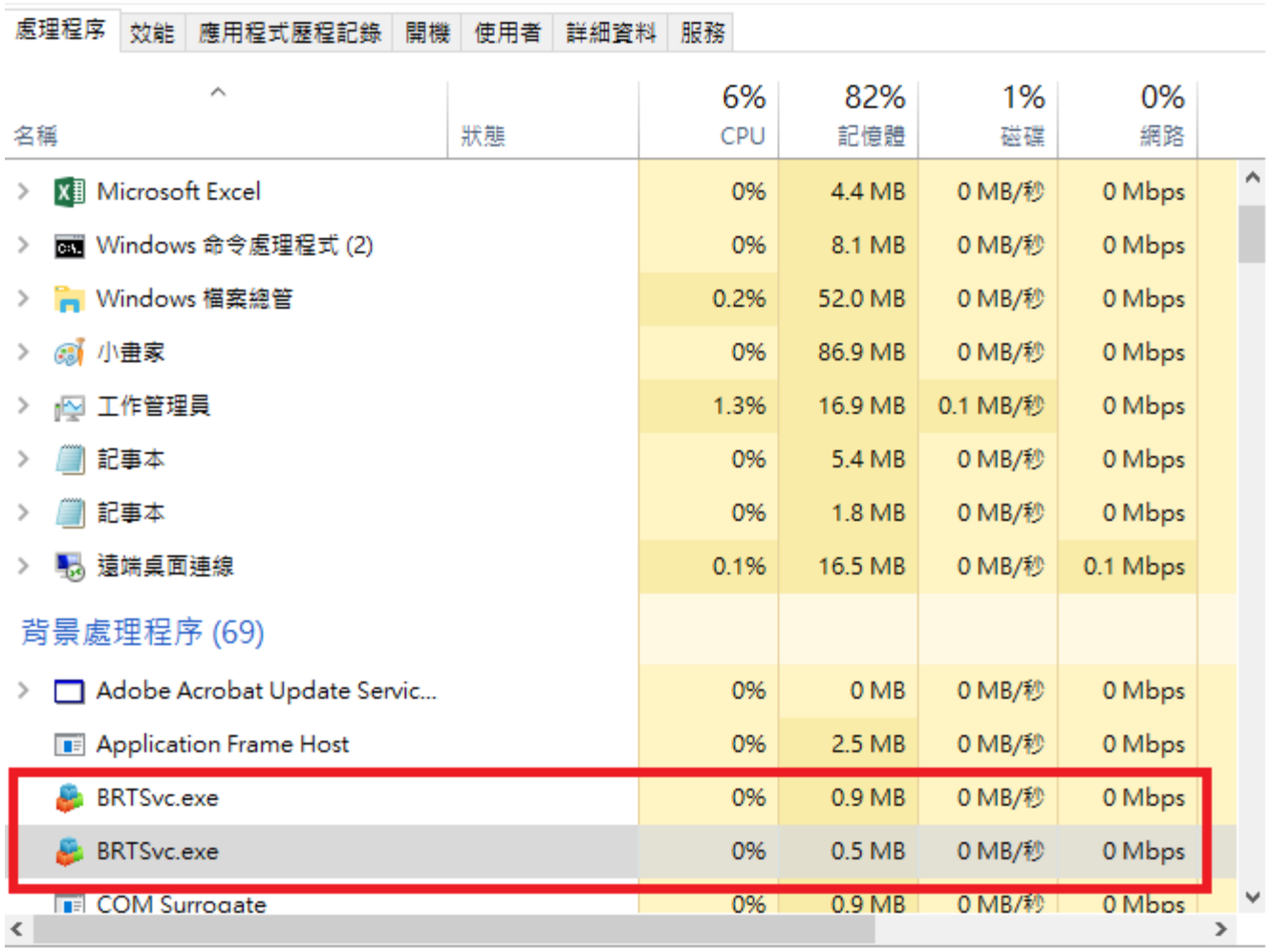
oCam 軟體挖礦事件

- 近期，收到轄下老師來信表示oCam 螢幕錄影程式，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。
- 如圖所示，oCam 安裝主程式的合約中，寫道會以挖礦程式做為贊助的方式，但使用者可以選擇贊助與否，話雖如此，但挖礦程式卻是**技術性**的預設打勾，只要一不注意，便開始贊助了。



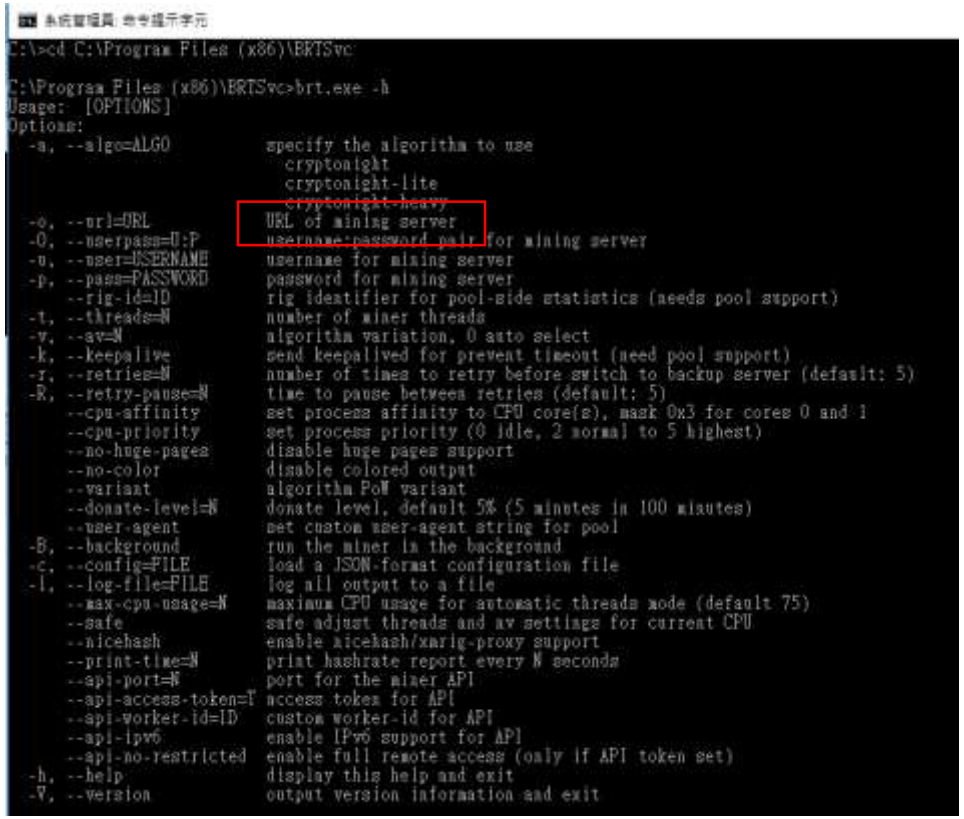
oCam 軟體挖礦事件

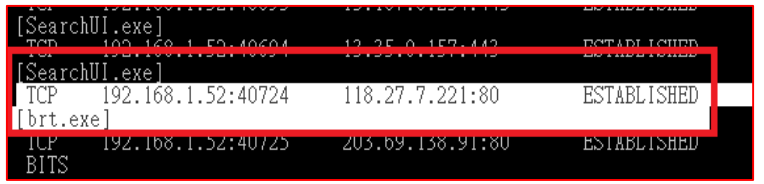
挖礦程式BRTSvc.exe本身不會有網路或是占用CUP的狀況，



oCam 軟體挖礦事件

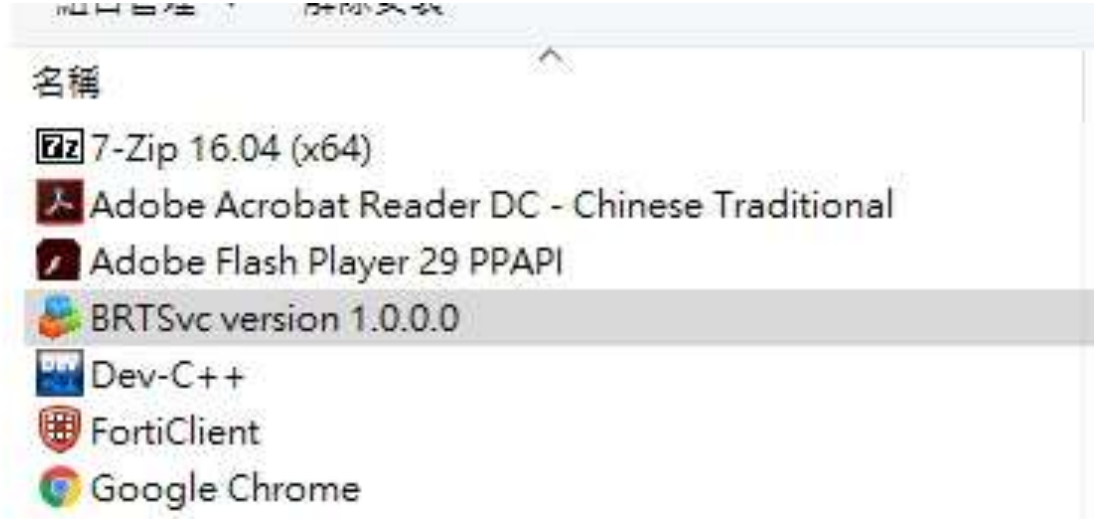
透過工作管理員的觀察，他實際上似乎是透過brt.exe，並且會連線到118.27.7.221:80 (此IP會隨者版本的更新而有所異動)





oCam 軟體挖礦事件

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



oCam 軟體挖礦事件

➢ 分析與建議

近期，因為挖礦軟體盛行，網站及軟體也開始以使用者協助挖礦的行為，作為贊助方式。北區ASOC目前已將挖礦Server ip 放入IPS進行偵測及阻擋。

針對此次oCam之挖礦程式，除使用者自行移除外，也可以再用下列有偵測到之防毒進行掃毒。