

資安事件宣導

挖礦程式

oCam螢幕錄影軟體暗藏BRTSvc挖礦程式

本校挖礦資安事件實際案例

- 近來各大學院校挖礦資安事件頻傳，引起臺灣學術網路危機處理中心高度關心，本校亦有相關案例發生（如下圖）

Summary

Destination Applications

 
 Monero.Cryptocurrency.Miner

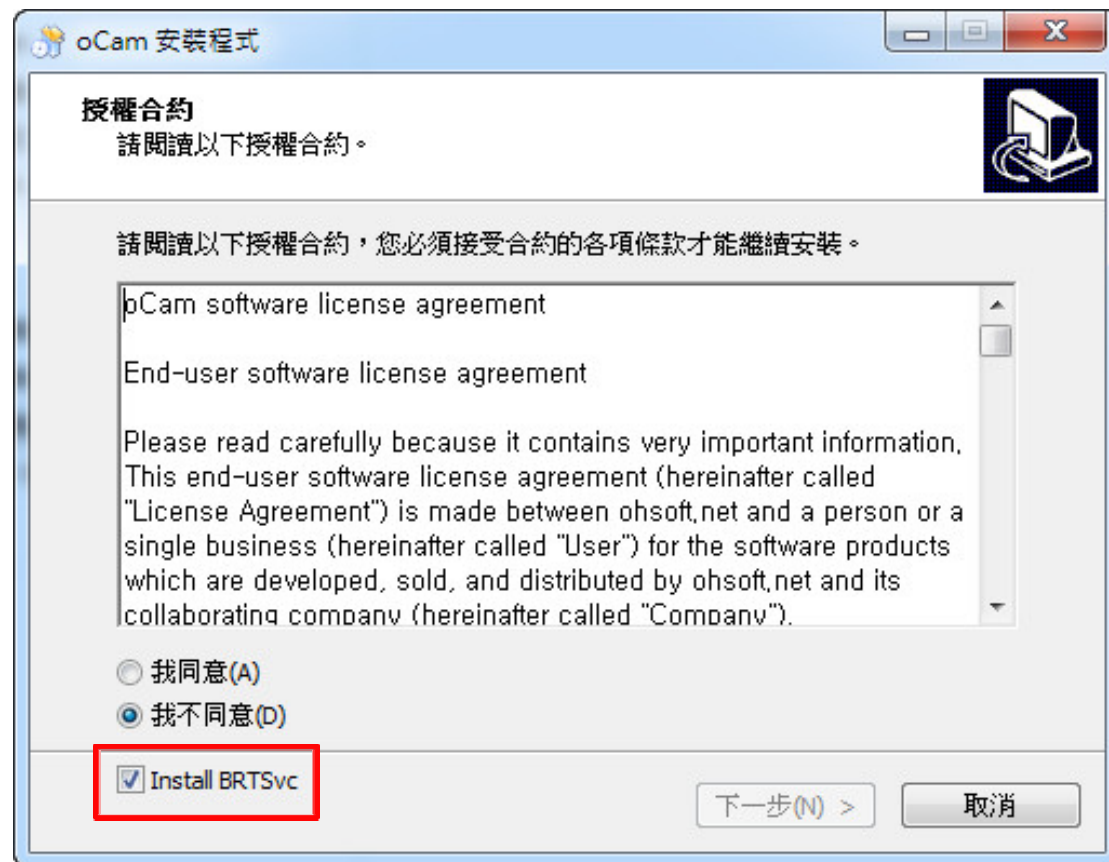
Application	Source	Threat	Session
#	Source	Source Interface	Device
1	140.123. 	port38	
2	140.123. 	port38	
3	140.123. 	port38	
4	140.123. 	port38	
5	140.123. 	port38	

何謂挖礦程式

- **挖礦程式**是近年興起的一種**惡意程式**，為了取得大量的運算資源，成為挖礦贏家以獲取利益，駭客利用各種管道散播挖礦程式，以取得被駭電腦的運算資源，致使**被駭電腦執行程式或瀏覽網站時明顯變慢**。
- 免費軟體在經費上對使用者具有很大的誘因，但是免費軟體也常會夾帶非使用者預期的程式，成為散播挖礦程式的管道之一。
- 此外，有些網站也可能被駭客植入挖礦腳本，駭客就可以利用使用者的瀏覽器來進行挖礦。

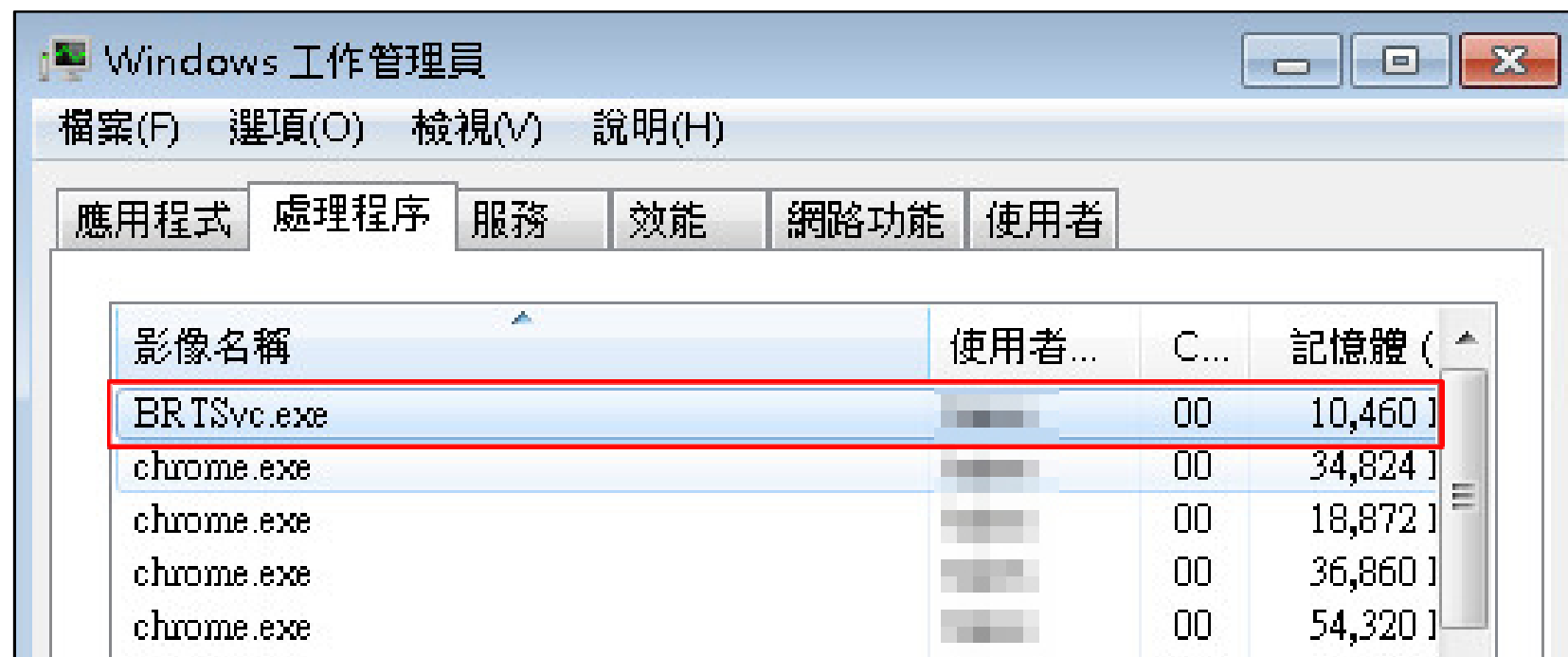
以 BRTSvc 挖礦程式為例(1/4)

- oCam是一款常見的螢幕錄影軟體，其安裝畫面暗藏安裝BRTSvc挖礦程式的選項，讓使用者不慎就把BRTSvc安裝到電腦中。



以 BRTSvc 挖礦程式為例(2/4)

- 被安裝 BRTSvc 的電腦，可以在工作管理員中看到其處理程序。



以 BRTSvc 挖礦程式為例(3/4)

- 萬一被安裝了 BRTSvc 挖礦程式，可以透過「解除安裝程式」來進行移除。
 - 開啟控制台，然後點選程式集底下的解除安裝程式



以 BRTSvc 挖礦程式為例(4/4)

- 找到 BRTSvc 並點擊兩下滑鼠左鍵，即可解除安裝。



防範方式(1/2)

- 安裝免費軟體時，務必要特別小心，仔細閱讀安裝過程的每一個畫面，如果發現有「搭便車」程式，除非能確定是必要的附加程式，否則就應取消勾選該程式的安裝，如此可以大幅降低被安裝挖礦病毒之類的惡意程式的機會。

防範方式(2/2)

- 建議瀏覽器可以安裝攔阻挖礦教本的擴充元件，例如：MinerBlock，亦可有效提高瀏覽網站的安全性。
 - ✓ [Chrome 擴充元件下載](#)
 - ✓ [IE 擴充元件下載](#)
 - ✓ [Firefox 擴充元件下載](#)

資料參考來源

- [挖礦\(數位貨幣\)](#)
- [oCam報告](#)
- [探討挖礦資安事件](#)
- [數以千計網站被植入挖礦軟體](#)