



區網會議

李墨軒

107.12.25.

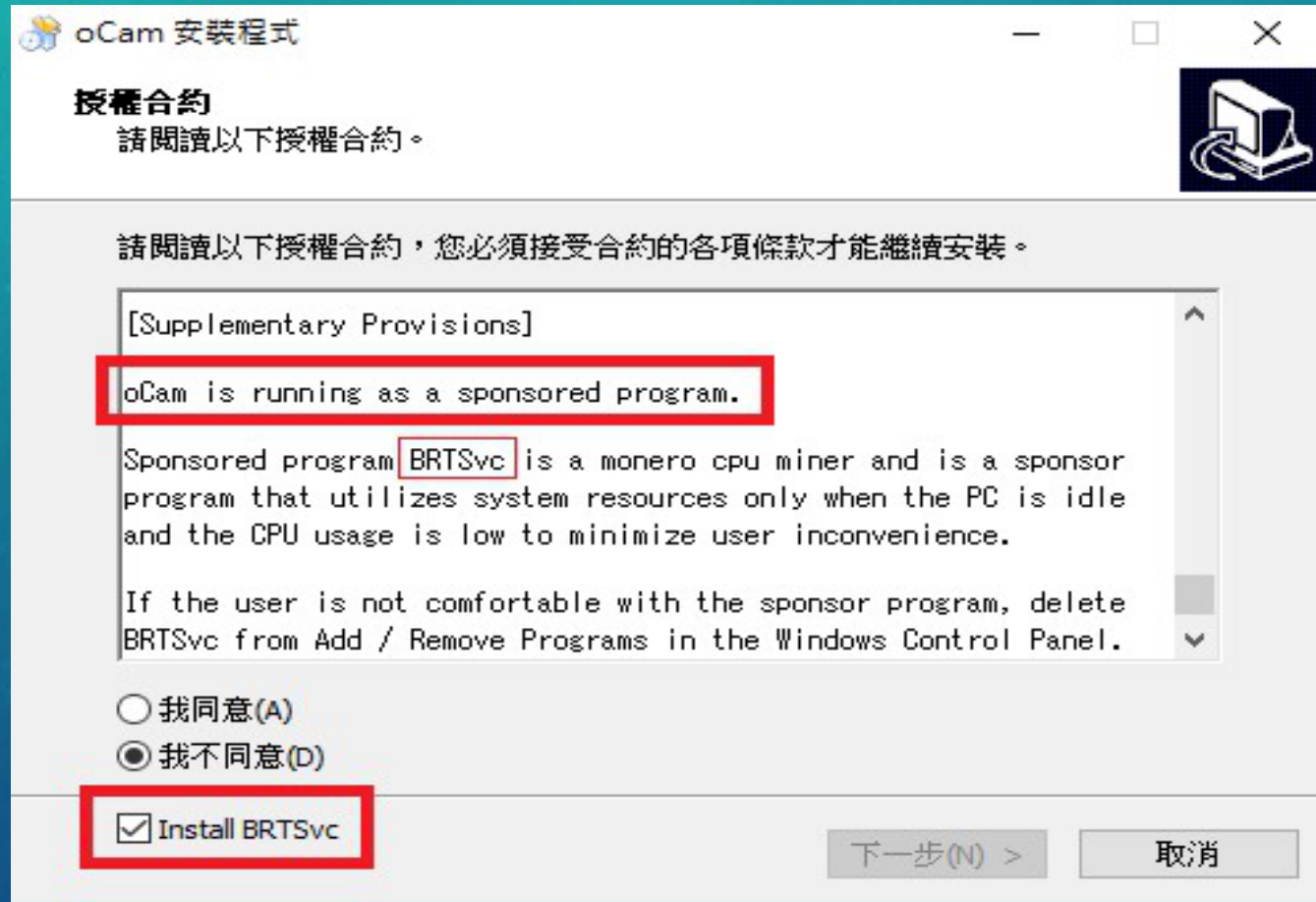
通報宣導

- 各級政府機關(構)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、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關(構)或關鍵資訊基礎設施運作，需橫向通知本會報關鍵資訊基礎設施安全管理組相關分組。

挖礦事件 - 1

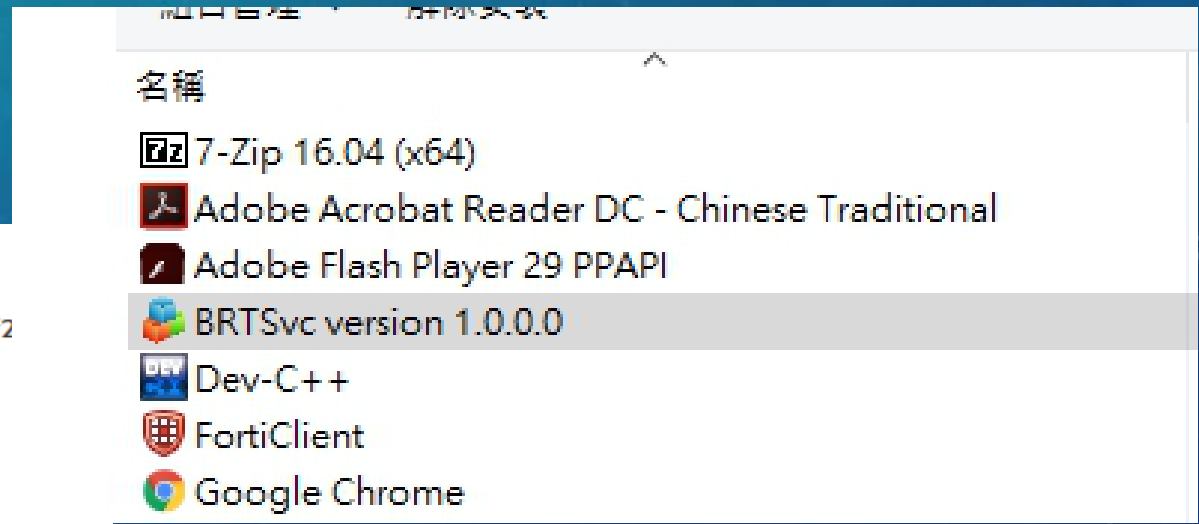
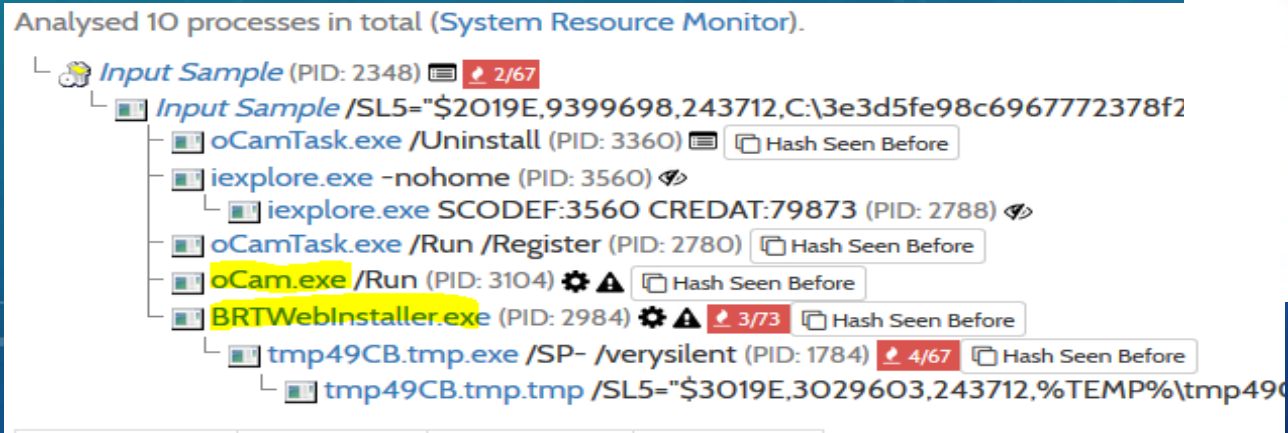
- 事件名稱：
 - PUA-OTHER Cryptocurrency Miner outbound connection attempt
- OCAM含有挖礦程式，經查測ohsoft旗下所有軟體(oCam、VirtualDVD、Secret Folder等)皆有此情況。

實際安裝之畫面



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/移除程式也即可順利移除。
- 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。



挖礦事件 - 2

- 事件名稱：
 - PUA-OTHER XMRig cryptocurrency mining pool connection attempt
- Bluestacks Android 模擬器，安裝程式疑似被植入挖礦。

官方說明

 **BlueStacks台灣** 11月27日上午11:33 · 🌐

【BlueStacks台灣 | #小藍 的教學時間】

哈囉！大家好，我是小藍，近期有幾位用戶反應發現他的BlueStacks有彈出惡意廣告，應用程式被自動刪除，被植入Test挖礦軟體等問題（從電腦的模擬器端口5.5.5.5植入），此問題在BlueStacks舊版本（沒有保持良好習慣）上和其他模擬器皆有可能發生，我們在上個月底已釋出安全性更新解決以上問題，強烈用戶建議至官網下載最新版本安裝。

🤔還有哪些方法提升裝置安全性呢？

提升裝置安全性您也可在BlueStacks和Android裝置開啟Google Play商店的「Play安全防護」保護裝置以及個人資料帳號安全。…… [更多](#)



開啟Play安全防護，保護BlueStacks以及帳號安全

 **BlueStacks台灣** 8月11日 · 🌐

【重要公告】

近日我們收到部分用戶以及小藍自己有遇到出現名為「Test應用（com.ufo.miner）」是一種數位貨幣挖礦程式被自動安裝到BlueStacks的Android中，這並非BlueStacks本身所安裝的應用，目前我們的相關人員正在處理此問題（將它加入黑名單），如果你電腦中防毒軟體偵測異常，請你在「系統應用-設置-應用程式」看看是否有此惡意軟體，如有發現請立即解除安裝，也強烈建議您在您的BlueStacks開啟Google Play商店中的「Play安全防護」保護BlueStacks以及個人資料帳號安全。

👉了解Play安全防護：https://www.android.com/intl/zh-TW_tw/play-protect

👉了解更多處理方法：https://www.reddit.com/.../8z8a.../avg_threat_name_elfmirairqtrj

BlueStacks臺灣粉絲專頁小藍 2018.08.11關心您
#BlueStacks #Android #GooglePlayProtect #Play安全防護



開啟Play安全防護，保護BlueStacks以及帳號安全

處理辦法

- 移除Bluestacks
- 更新到最新版本

END