

**【資安通報】oCam 教學螢幕錄影程式藏有挖礦程式「BRTSvc」！**

● 原由：oCam 安裝程式內嵌軟體商 OHSOFT 贊助挖礦程式 BRTSvc。

● 安裝注意：

1. 在安裝主程式的「合約內容」頁面中有寫明《在安裝或更新時使用者可以安裝贊助軟體》，且在安裝時已預設打勾同意同步進行礦程式- BRTSvc 安裝，往往使用者都會忽略直接點按【下一步】執行安裝，就把挖礦程式也安裝到電腦中。

oCam 安裝程式

授權合約  
請閱讀以下授權合約。

請閱讀以下授權合約，您必須接受合約的各項條款才能繼續安裝。

oCam software license agreement

End-user software license agreement

Please read carefully because it contains very important information. This end-user software license agreement (hereinafter called "License Agreement") is made between ohsoft.net and a person or a single business

我同意(A)

我不同意(D)

Install BRTSvc

此處的 Install BRTSvc 即為安裝挖礦程式的選項請務必將其勾拿掉

取消

系統預設打勾同步安裝挖礦程式 BRTSvc

請留心手動取消勾選，不同意安裝挖礦程式 BRTSvc

2. 不經意下安裝挖礦程式 BRTSvc 狀態

若是安裝時不小心安裝了，當執行 oCam 軟體時，BRTSvc 會在系統背景中執行，可以進入工作管理員(進入方式 CTRL+ALT+DEL 選擇工作管理員) 進行確認。

工作管理員

名稱	狀態	37% CPU	75% 記憶體	0% 磁碟	0% 網路
ASUS Software Manager		0%	1.6 MB	0 MB/秒	0 Mbps
ASUS Software Manager Agent		0%	2.5 MB	0 MB/秒	0 Mbps
ASUS System Analysis		0%	0.6 MB	0 MB/秒	0 Mbps
ASUS System Diagnosis		0%	0.1 MB	0 MB/秒	0 Mbps
Bonjour Service		0%	0.7 MB	0 MB/秒	0 Mbps
BRTSvc.exe		0%	1.7 MB	0 MB/秒	0 Mbps
BRTSvc.exe		0%	1.2 MB	0 MB/秒	0 Mbps

```

/ TOR outside:01.220.9.207/29025 (01.220.9.207/29025) to DMZ:140.129.251.1/53 (140.129
outside:203.160.250.60/80 to inside:140.129.253.33/44384 duration 0:00:00 bytes 422
3 for outside:61.220.11.79/27425 (61.220.11.79/27425) to DMZ:140.129.251.1/53 (140.1
9 for outside:61.220.11.28/26068 (61.220.11.28/26068) to DMZ:140.129.251.1/53 (140.1
outside:168.95.192.1/53 to inside:140.129.255.2/54902 duration 0:00:00 bytes 102
ide:10.131.4.68/1531 to outside:140.129.251.253/1531
50 for outside:104.207.150.205/443 (104.207.150.205/443) to inside:10.131.4.68/1531
1 for outside:61.220.9.186/39825 (61.220.9.186/39825) to DMZ:140.129.251.1/53 (140.1
.166/27022 to outside10M:122.146.6.158/3756
2 for outside:61.220.11.151/21859 (61.220.11.151/21859) to DMZ:140.129.251.1/53 (140
outside:147.02.146.121/442 to inside:172.27.1.14/52204 duration 0:01:01 bytes 35665
    
```

背景執行 BRTSvs 程式進行挖礦行為

透過網管程式顯示，使用者電腦自動會透過 brt.exe 連線到 104.207.150.205:443 (此 IP 會隨著版本的更新而有所異動)

● 如何移除已裝之挖礦程式 BRTSvs

1. 若需移除挖礦程式 BRTSvc 時，必須單獨移除，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。

2. BRTSvc 挖礦程式不會隨者主程式移除而移除，進入控制台 > 程式集 >> 程式和功能，將 BRTSvc 移除安裝即可。

程式和功能

← → ↓ ↑ 控制台 > 程式集 >> 程式和功能

控制台首頁

解除安裝或變更程式

檢視已安裝的更新

若要解除安裝程式，請從清單選取程式，然後按一下 [解除安裝]、[變更] 或 [修復]。

開啟或關閉 Windows 功能

名稱	解除安裝	發行者
7-Zip 19.00 (x64)		Igor Pavlov
Adobe Acrobat Reader DC - Chinese Traditional		Adobe Systems Incorporated
AnyDesk		philandro Software GmbH
Bonjour		Apple Inc.
BRTSvc version 1.0.0.0	解除安裝(U)	
Cisco ASDM IDM Launcher		
EPSON印表機軟體		
Google Chrome		Google LLC



● 重要提醒與建議

1. 請下載乾淨最新版之 oCam 軟體使用，下載網址 <https://lic.tumt.edu.tw/files/13-1025-567.php>。

2. 網路上部份免費軟體都會找贊助商贊助，進而也連帶將挖礦程式就會隱身其中，利用使用者在使用軟體時協助挖礦，請各位使用者在使用時務必注意是否有將挖礦程式移除。