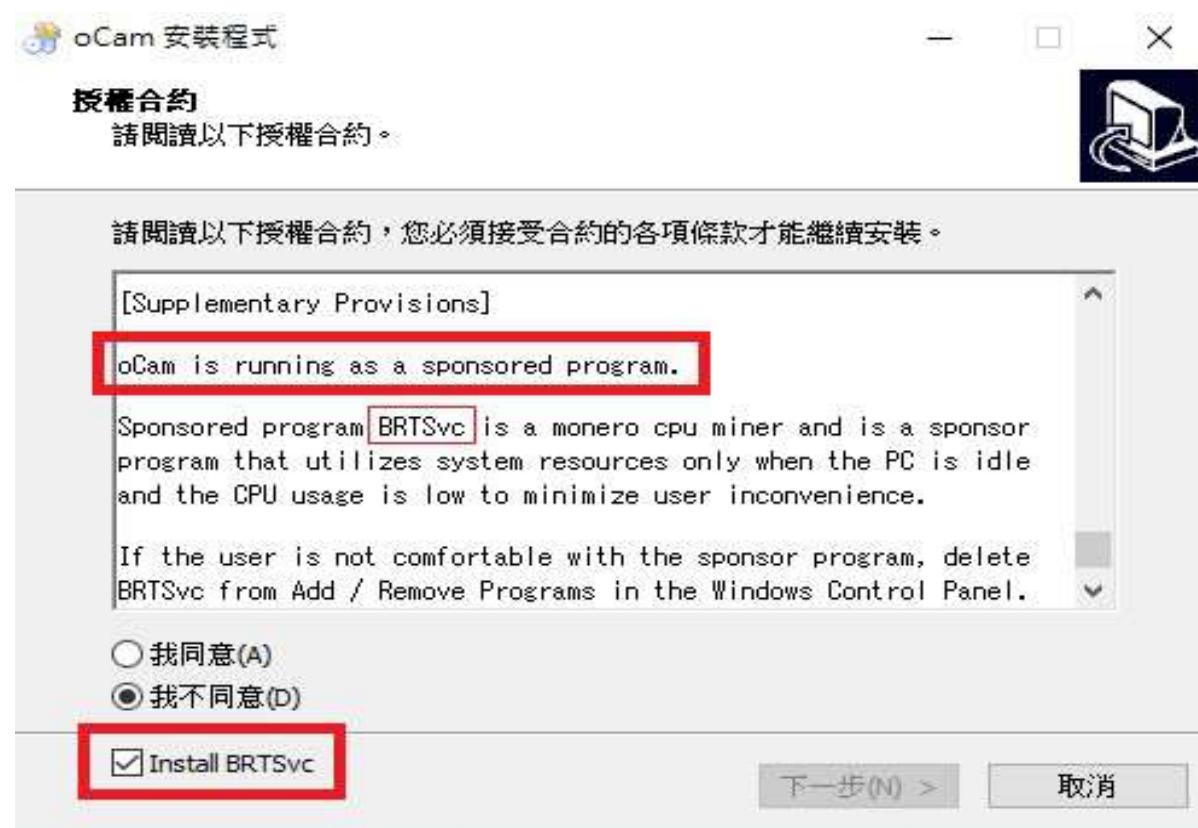


Ocam報告

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，

遠端程序						
效能 應用程式歷程記錄 開機 使用者 詳細資料 服務						
名稱	狀態	6% CPU	82% 記憶體	1% 磁碟	0% 網路	
> Microsoft Excel		0%	4.4 MB	0 MB/秒	0 Mbps	
> Windows 命令處理程式 (2)		0%	8.1 MB	0 MB/秒	0 Mbps	
> Windows 檔案總管		0.2%	52.0 MB	0 MB/秒	0 Mbps	
> 小畫家		0%	86.9 MB	0 MB/秒	0 Mbps	
> 工作管理員		1.3%	16.9 MB	0.1 MB/秒	0 Mbps	
> 記事本		0%	5.4 MB	0 MB/秒	0 Mbps	
> 記事本		0%	1.8 MB	0 MB/秒	0 Mbps	
> 遠端桌面連線		0.1%	16.5 MB	0 MB/秒	0.1 Mbps	
背景處理程序 (69)						
> Adobe Acrobat Update Servic...		0%	0 MB	0 MB/秒	0 Mbps	
Application Frame Host		0%	2.5 MB	0 MB/秒	0 Mbps	
BRTSvc.exe		0%	0.9 MB	0 MB/秒	0 Mbps	
BRTSvc.exe		0%	0.5 MB	0 MB/秒	0 Mbps	
COM Surrogate		0%	0.9 MB	0 MB/秒	0 Mbps	

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)

```

C:\>cd C:\Program Files (x86)\BERTSvc
C:\Program Files (x86)\BERTSvc>brt.exe -h
Usage: [OPTIONS]
Options:
-a, --algo=ALGO          specify the algorithm to use
                        cryptonight
                        cryptonight-lite
                        cryptonight-heavy
-o, --url=URL            URL of mining server
-u, --user=USERNAME     username:password pair for mining server
-p, --pass=PASSWORD     password for mining server
--rig-id=ID             rig identifier for pool-side statistics (needs pool support)
-t, --threads=N         number of miner threads
-v, --av=N              algorithm variation, 0 auto select
-k, --keepalive         send keepalives for prevent timeout (need pool support)
-r, --retries=N         number of times to retry before switch to backup server (default: 5)
-R, --retry-pause=N     time to pause between retries (default: 5)
--cpu-affinity          set process affinity to CPU core(s), mask 0x3 for cores 0 and 1
--cpu-priority          set process priority (0 idle, 2 normal to 5 highest)
--no-huge-pages        disable huge pages support
--no-color             disable colored output
--variant              algorithm PoW variant
--donate-level=N       donate level, default 5% (5 minutes in 100 minutes)
--user-agent            set custom user-agent string for pool
-B, --background       run the miner in the background
-c, --config=FILE      load a JSON-format configuration file
-l, --log-file=FILE    log all output to a file
--max-cpu-usage=N      maximum CPU usage for automatic threads mode (default 75)
--safe                 safe adjust threads and av settings for current CPU
--nicehash             enable nicehash/xmrig-proxy support
--print-time=N        print hashrate report every N seconds
--api-port=N           port for the miner API
--api-access-token=T   access token for API
--api-worker-id=ID     custom worker-id for API
--api-ipv6             enable IPv6 support for API
--api-no-restricted   enable full remote access (only if API token set)
-h, --help             display this help and exit
-V, --version          output version information and exit

```

[SearchUI.exe]	TCP	192.168.1.52:40604	118.27.7.221:80	ESTABLISHED
[SearchUI.exe]	TCP	192.168.1.52:40724	118.27.7.221:80	ESTABLISHED
[brt.exe]	TCP	192.168.1.52:40725	205.69.138.91:80	ESTABLISHED
BITS				

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。

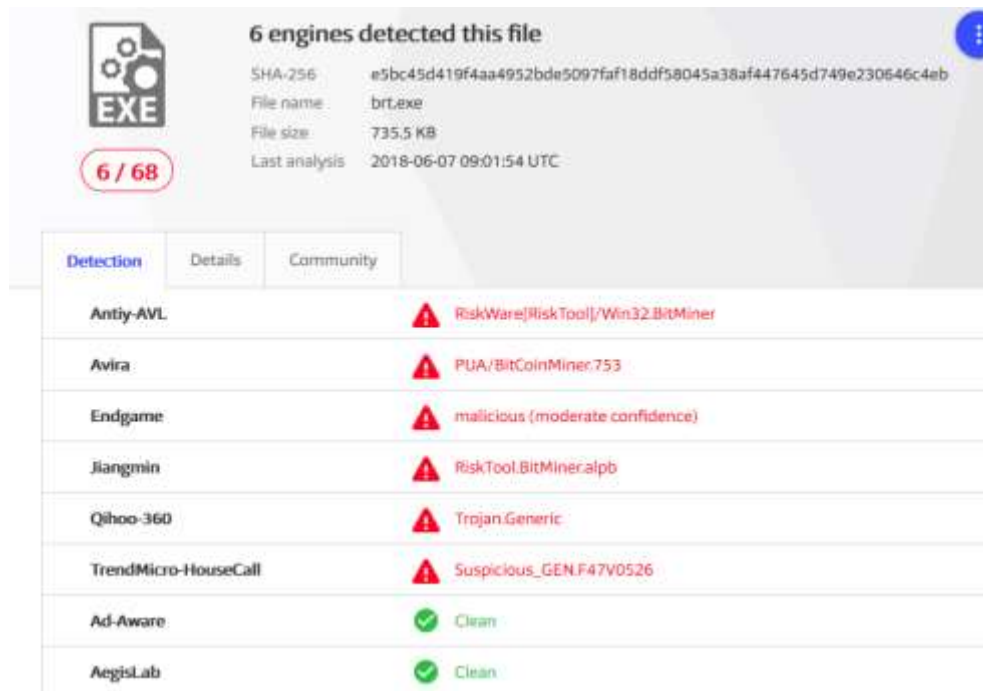


oCam 軟體挖礦事件

➤ 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。



6 engines detected this file

SHA-256: e5bc45d419f4aa4952bde5097faf18ddf58045a38af447645d749e230646c4eb
File name: brt.exe
File size: 735.5 KB
Last analysis: 2018-06-07 09:01:54 UTC

6 / 68

Detection	Details	Community
Antiy-AVL		⚠ RiskWare[RiskTool]/Win32.BitMiner
Avira		⚠ PUA/BitCoinMiner.753
Endgame		⚠ malicious (moderate confidence)
Jiangmin		⚠ RiskTool.BitMiner.alpb
Qihoo-360		⚠ Trojan.Generic
TrendMicro-HouseCall		⚠ Suspicious_GEN.F47V0526
Ad-Aware		✅ Clean
AegisLab		✅ Clean