

# ASOC

# 事件分析

台大ASOC 2/1

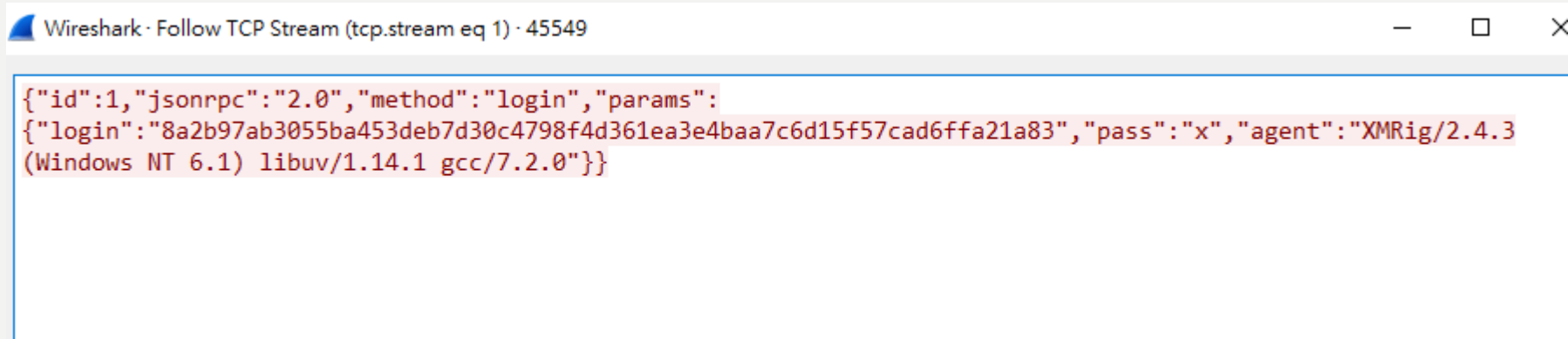
# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION [挖礦惡意軟體]

- 近期發現有不少挖礦相關事件，如下：

線		connection	午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 09:49:42 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 09:51:14 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 09:57:03 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 10:22:48 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 10:35:10 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 11:09:10 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 11:23:21 上午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 01:33:40 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 01:36:51 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 01:37:29 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 01:38:03 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 02:25:17 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 02:52:27 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 02:59:09 下午
主機進行惡意程式連	處理完畢	MALWARE-CNC Win.Trojan.CoinMiner outbound connection	01/26/2018 03:08:22 下午

# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION 【挖礦惡意軟體】

- 經ASOC分析所擷取的封包後，發現這類事件的封包皆傳送特定”json”格式內容之封包，如下圖：

A screenshot of a Wireshark window titled "Wireshark - Follow TCP Stream (tcp.stream eq 1) - 45549". The window displays a JSON payload in a text area. The JSON content is: {"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"8a2b97ab3055ba453deb7d30c4798f4d361ea3e4baa7c6d15f57cad6ffa21a83","pass":"x","agent":"XMRig/2.4.3 (Windows NT 6.1) libuv/1.14.1 gcc/7.2.0"}}. The text is highlighted in a light red color.

```
Wireshark - Follow TCP Stream (tcp.stream eq 1) - 45549  
{"id":1,"jsonrpc":"2.0","method":"login","params":  
{"login":"8a2b97ab3055ba453deb7d30c4798f4d361ea3e4baa7c6d15f57cad6ffa21a83","pass":"x","agent":"XMRig/2.4.3  
(Windows NT 6.1) libuv/1.14.1 gcc/7.2.0"}}
```

# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION 【挖礦惡意軟體】

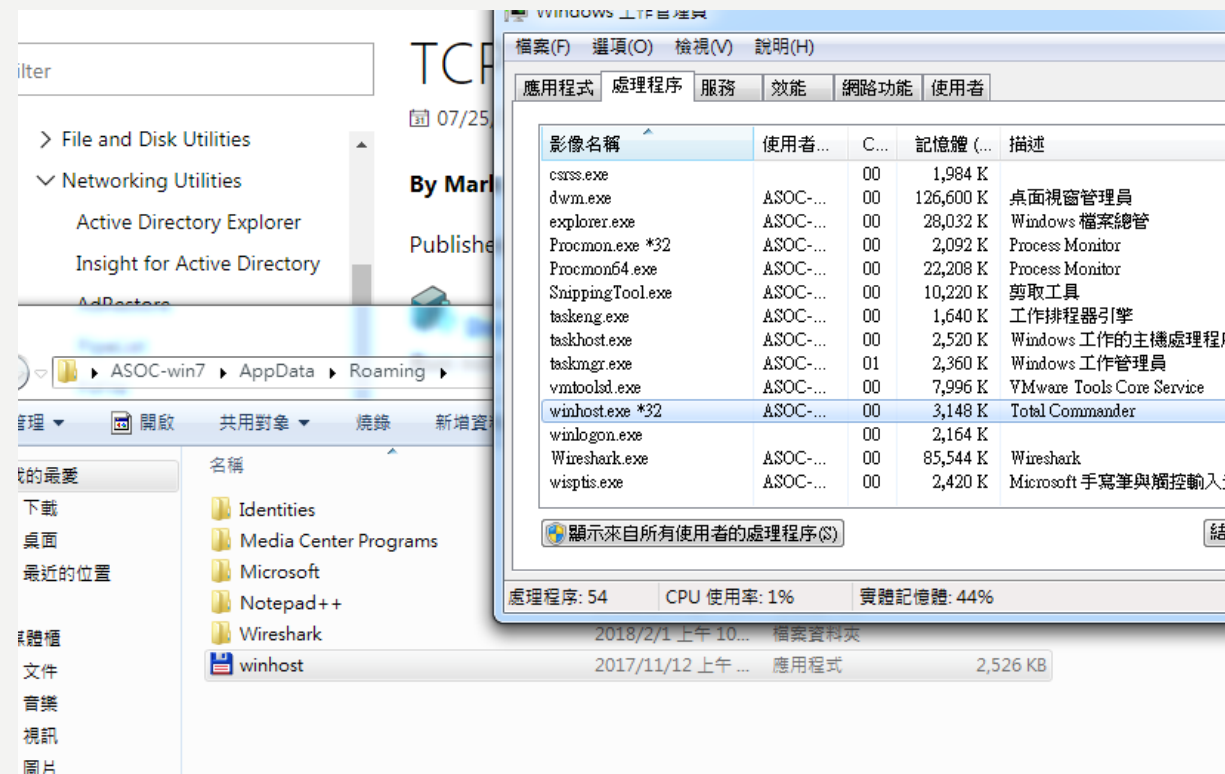
- 經調查後，發現上述封包之特徵為數位貨幣 – 門羅幣 (XMR) 的挖礦程式所有，相關架設門羅幣挖礦伺服器資訊，如下網址：<https://github.com/xmrig/xmrig>



安全、保護隱私且完全匿蹤的加密貨幣

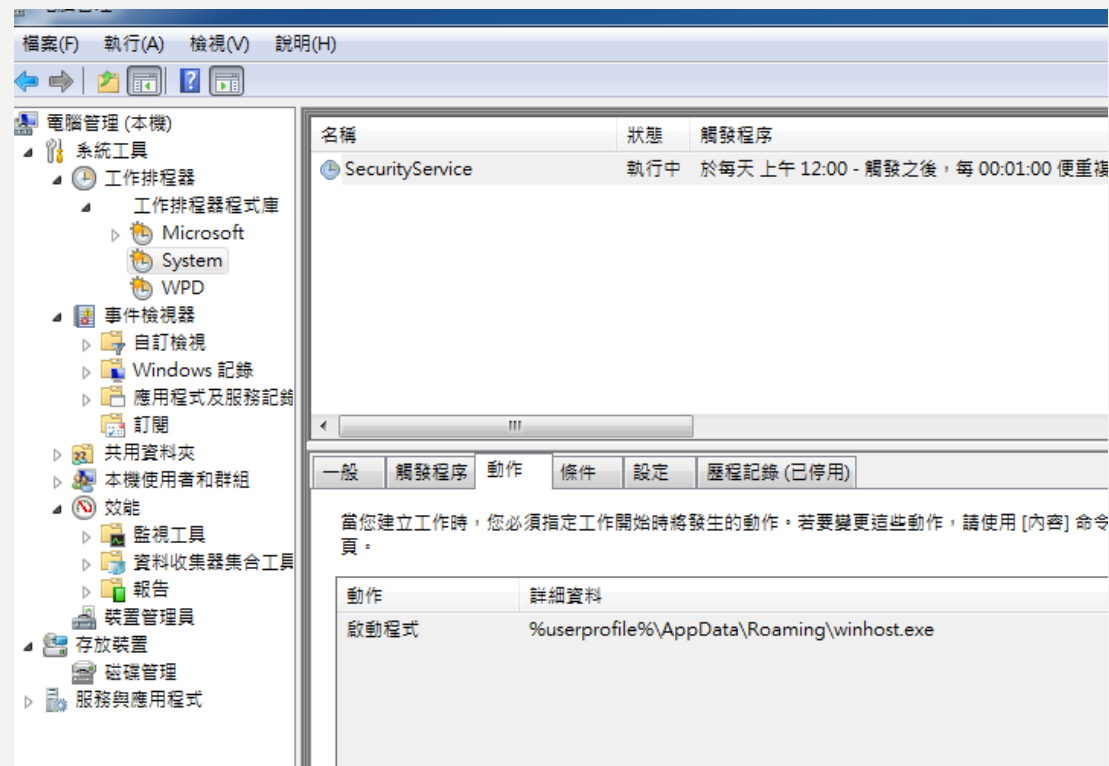
# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION [挖礦惡意軟體]

- 當挖礦程式被製作成惡意軟體時，即可綁架無辜使用者的電腦，並且自動執行於背景中，幫助攻擊者進行CPU挖礦。



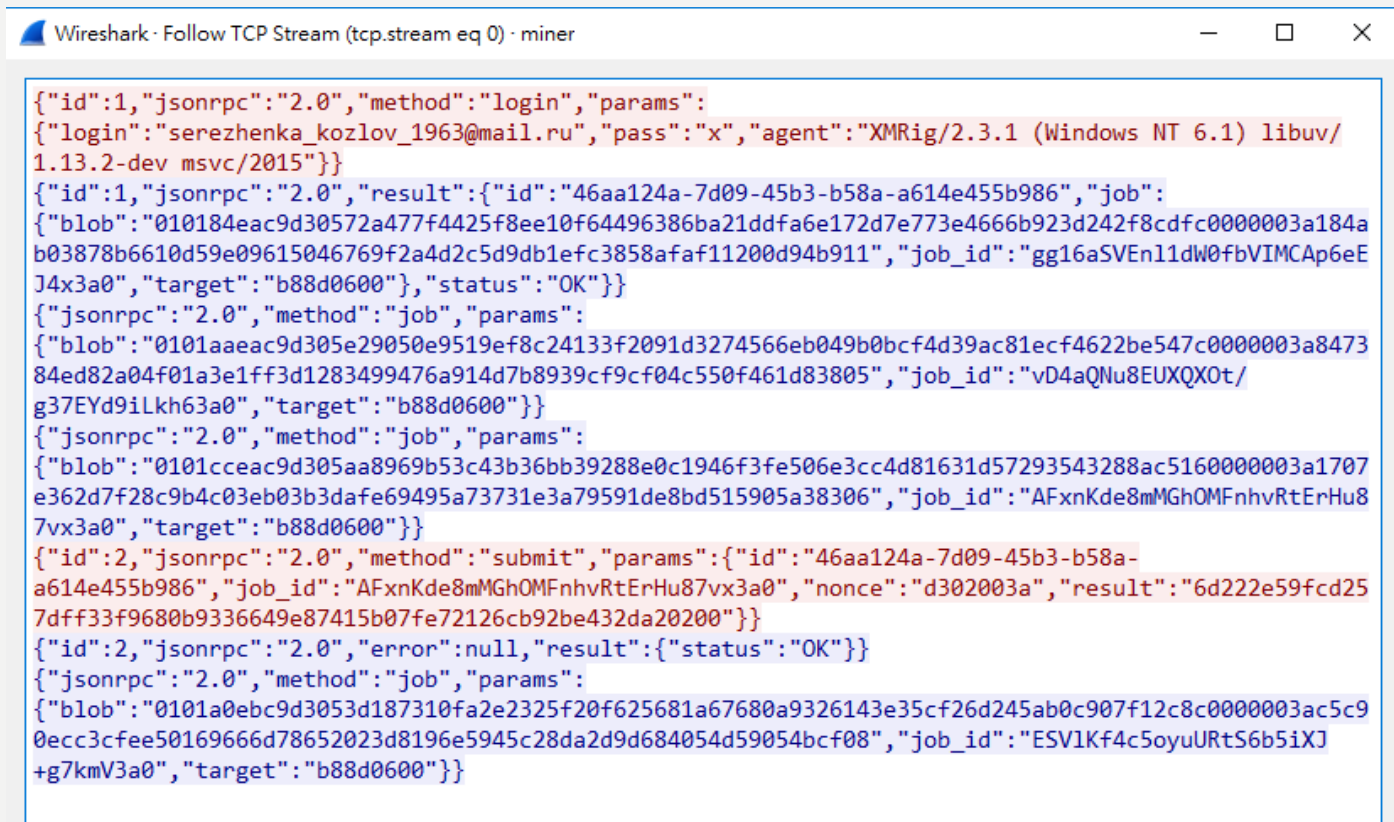
# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION [挖礦惡意軟體]

- 如ASOC搜集到的惡意軟體樣本，更會自動設定排程，常駐於使用者電腦，如下圖：



# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION [挖礦惡意軟體]

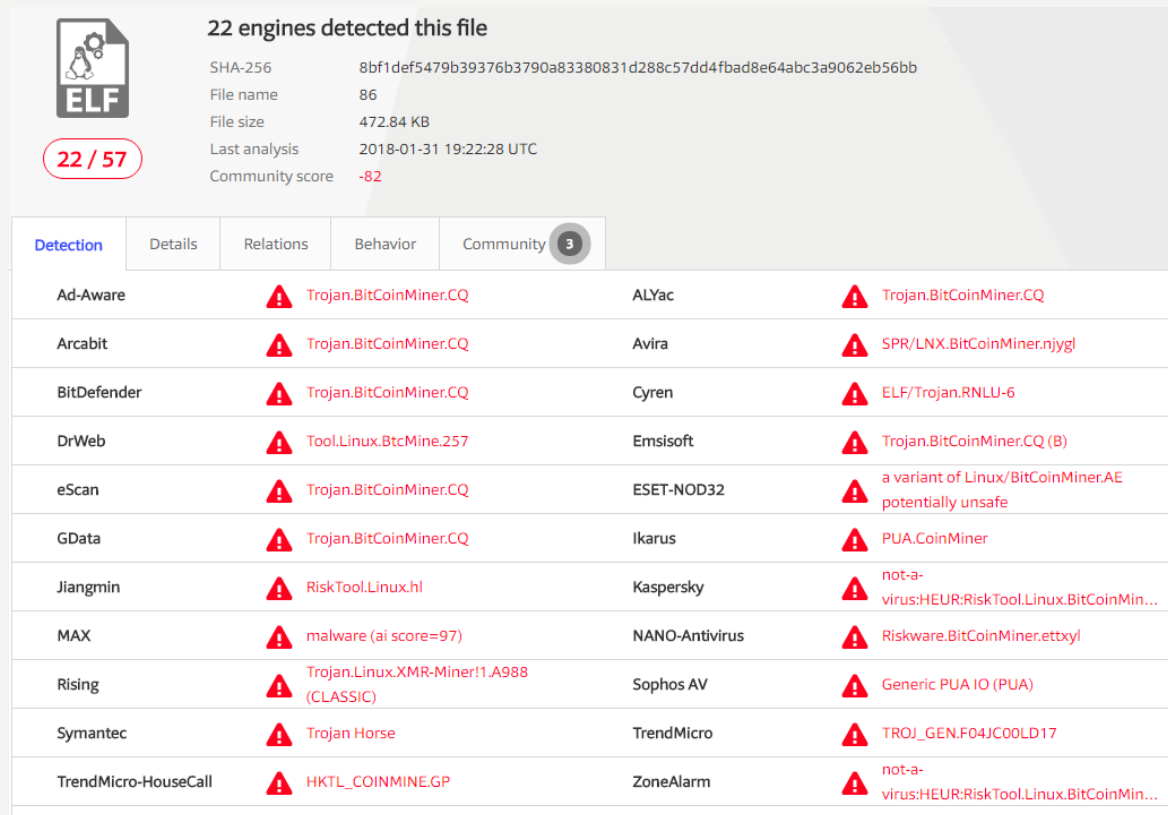
- 從側錄的封包中，我們可以發現惡意軟體正在向挖礦主機進行報到登入及其他通信動作，如下圖：



```
Wireshark - Follow TCP Stream (tcp.stream eq 0) - miner
{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"serezhenka_kozlov_1963@mail.ru","pass":"x","agent":"XMRig/2.3.1 (Windows NT 6.1) libuv/
1.13.2-dev msvc/2015"}}
{"id":1,"jsonrpc":"2.0","result":{"id":"46aa124a-7d09-45b3-b58a-a614e455b986","job":
{"blob":"010184eac9d30572a477f4425f8ee10f64496386ba21ddfa6e172d7e773e4666b923d242f8cdfc000003a184a
b03878b6610d59e09615046769f2a4d2c5d9db1efc3858afaf11200d94b911","job_id":"gg16aSVEn11dW0fbVIMCAp6eE
J4x3a0","target":"b88d0600"},"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0101aaeac9d305e29050e9519ef8c24133f2091d3274566eb049b0bcf4d39ac81ecf4622be547c000003a8473
84ed82a04f01a3e1ff3d1283499476a914d7b8939cf9cf04c550f461d83805","job_id":"vD4aQNu8EUXQX0t/
g37EYd9iLkh63a0","target":"b88d0600"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0101ccea9d305aa8969b53c43b36bb39288e0c1946f3fe506e3cc4d81631d57293543288ac516000003a1707
e362d7f28c9b4c03eb03b3dafef69495a73731e3a79591de8bd515905a38306","job_id":"AFxnKde8mMGhOMFnhvRtErHu8
7vx3a0","target":"b88d0600"}}
{"id":2,"jsonrpc":"2.0","method":"submit","params":{"id":"46aa124a-7d09-45b3-b58a-
a614e455b986","job_id":"AFxnKde8mMGhOMFnhvRtErHu87vx3a0","nonce":"d302003a","result":"6d222e59fcd25
7dff33f9680b9336649e87415b07fe72126cb92be432da20200"}}
{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0101a0ebc9d3053d187310fa2e2325f20f625681a67680a9326143e35cf26d245ab0c907f12c8c000003ac5c9
0ecc3cfee50169666d78652023d8196e5945c28da2d9d684054d59054bcf08","job_id":"ESV1Kf4c5oyuURtS6b5iXJ
+g7kmV3a0","target":"b88d0600"}}
```

# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION [挖礦惡意軟體]

以上挖礦惡意程式，大部分防毒軟體皆有特徵馬能夠偵測到，如下：



22 engines detected this file

SHA-256 8bf1def5479b39376b3790a83380831d288c57dd4fbad8e64abc3a9062eb56bb  
File name 86  
File size 472.84 KB  
Last analysis 2018-01-31 19:22:28 UTC  
Community score -82

22 / 57

Detection	Details	Relations	Behavior	Community
Ad-Aware	Trojan.BitCoinMiner.CQ	ALYac	Trojan.BitCoinMiner.CQ	
Arcabit	Trojan.BitCoinMiner.CQ	Avira	SPR/LNX.BitCoinMiner.njygl	
BitDefender	Trojan.BitCoinMiner.CQ	Cyren	ELF/Trojan.RNLU-6	
DrWeb	Tool.Linux.BtcMine.257	Emsisoft	Trojan.BitCoinMiner.CQ (B)	
eScan	Trojan.BitCoinMiner.CQ	ESET-NOD32	a variant of Linux/BitCoinMiner.AE potentially unsafe	
GData	Trojan.BitCoinMiner.CQ	Ikarus	PUA.CoinMiner	
Jiangmin	RiskTool.Linux.hl	Kaspersky	not-a-virus:HEUR:RiskTool.Linux.BitCoinMin...	
MAX	malware (ai score=97)	NANO-Antivirus	Riskware.BitCoinMiner.ettxyl	
Rising	Trojan.Linux.XMR-Miner!1.A988 (CLASSIC)	Sophos AV	Generic PUA IO (PUA)	
Symantec	Trojan Horse	TrendMicro	TROJ_GEN.F04JC00LD17	
TrendMicro-HouseCall	HKTL_COINMINE.GP	ZoneAlarm	not-a-virus:HEUR:RiskTool.Linux.BitCoinMin...	



# MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION 【挖礦惡意軟體】

- 建議及緩解方法

因下載程式已遭各家防毒軟體認定為惡意程式，建議遭告警的使用者，盡速使用防毒軟體掃描並清除，或是利用以下所提供之惡意軟體清除程式掃毒：

- ✓ <https://downloads.malwarebytes.com/file/mb3/>

- ✓ <https://security.symantec.com/nbrt/npe.aspx?&NUCLANG=zh-tw>