ASOC
事件分析

台大ASOC 2/1

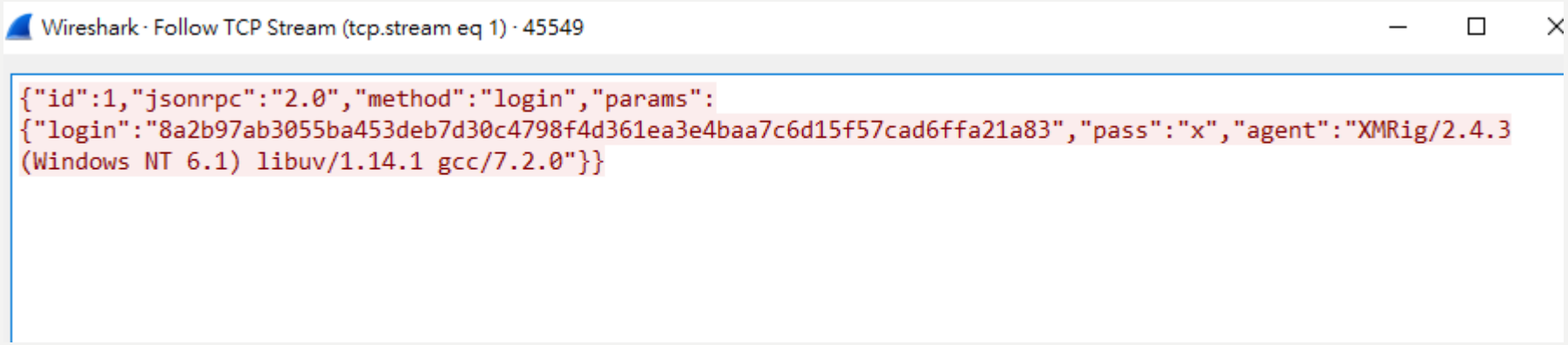
MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION【挖礦惡意軟體】

- 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線	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線	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線	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線	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線	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線	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線	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線	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線	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線	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線	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線	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線	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線	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線	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：

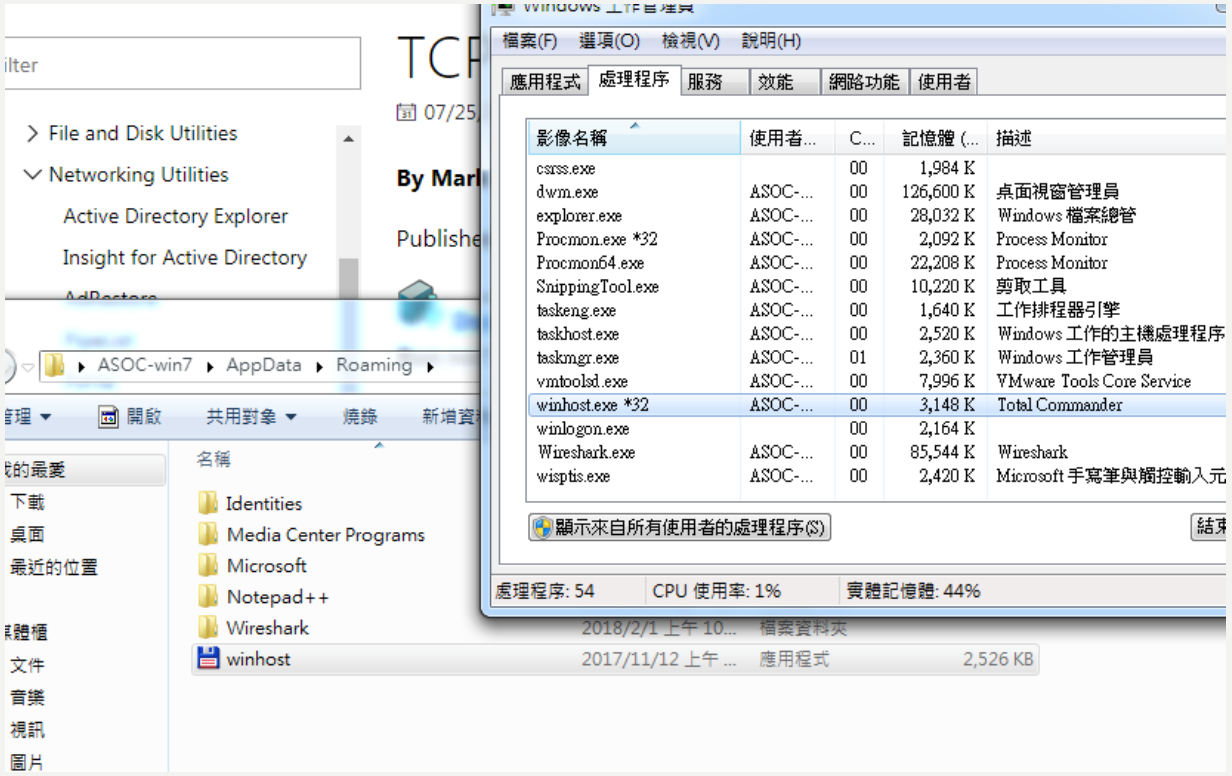


MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION【挖礦惡意軟體】

- 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

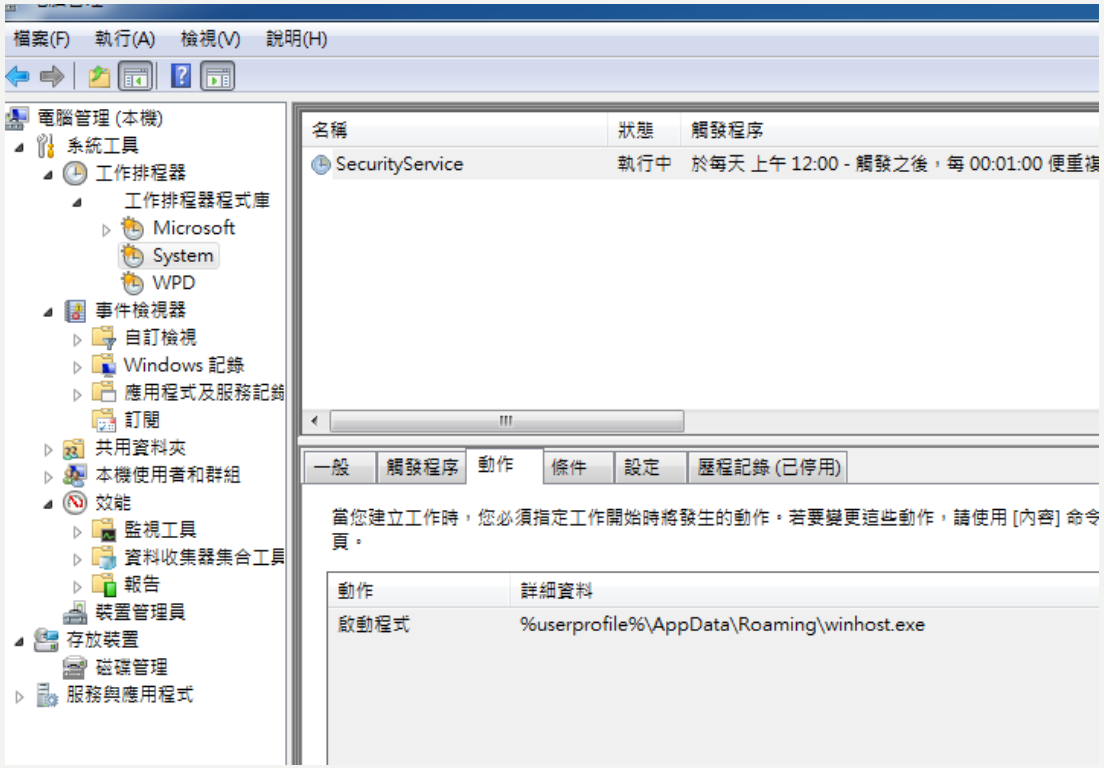
MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION【挖礦惡意軟體】

- 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。



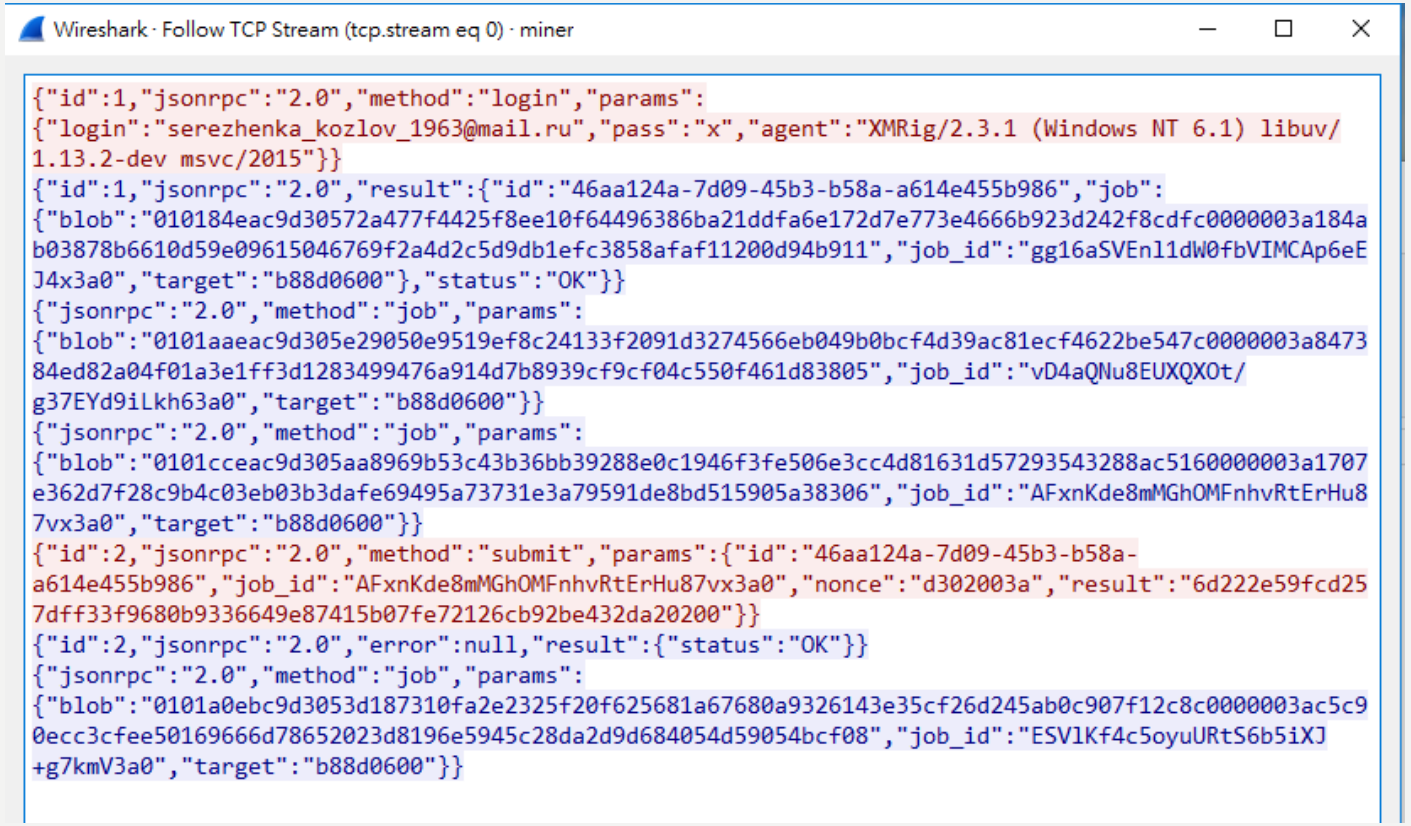
MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION【挖礦惡意軟體】

- 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：



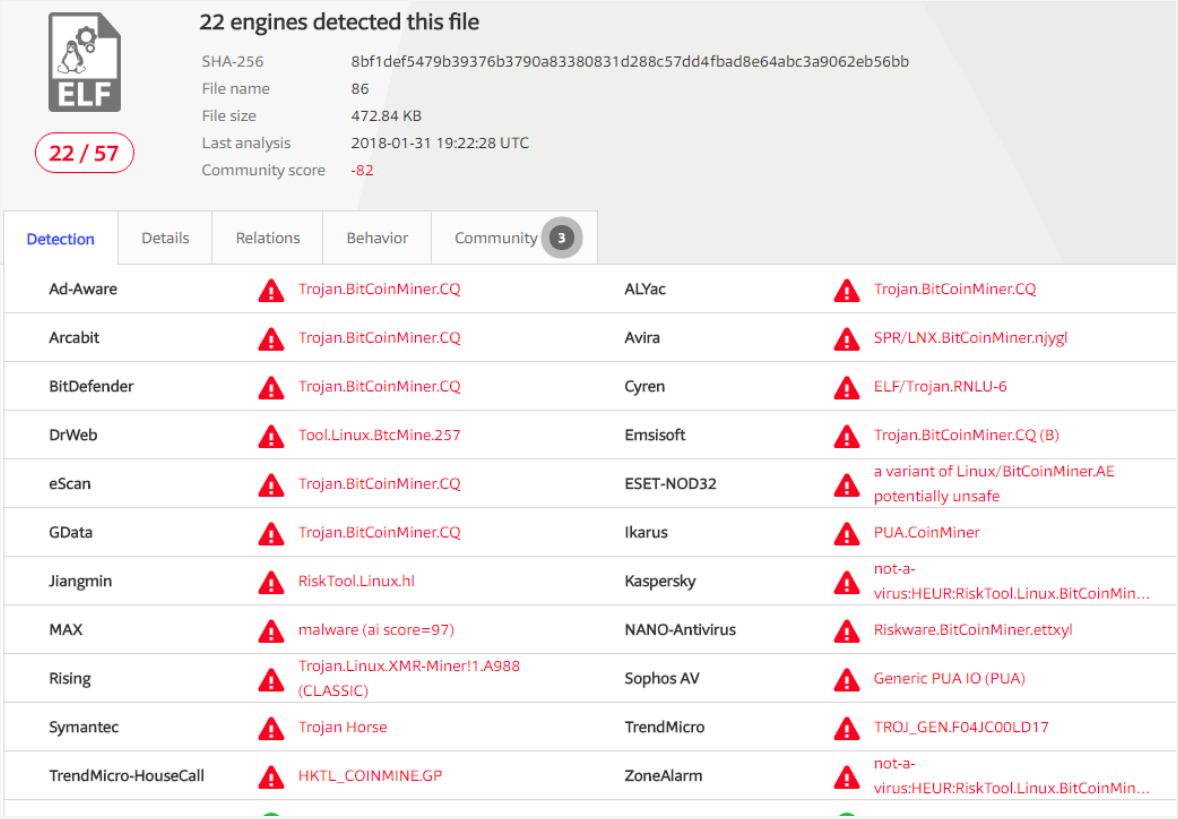
MALWARE-CNC WIN.TROJAN.COINMINER OUTBOUND CONNECTION【挖礦惡意軟體】

- 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：



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 3

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