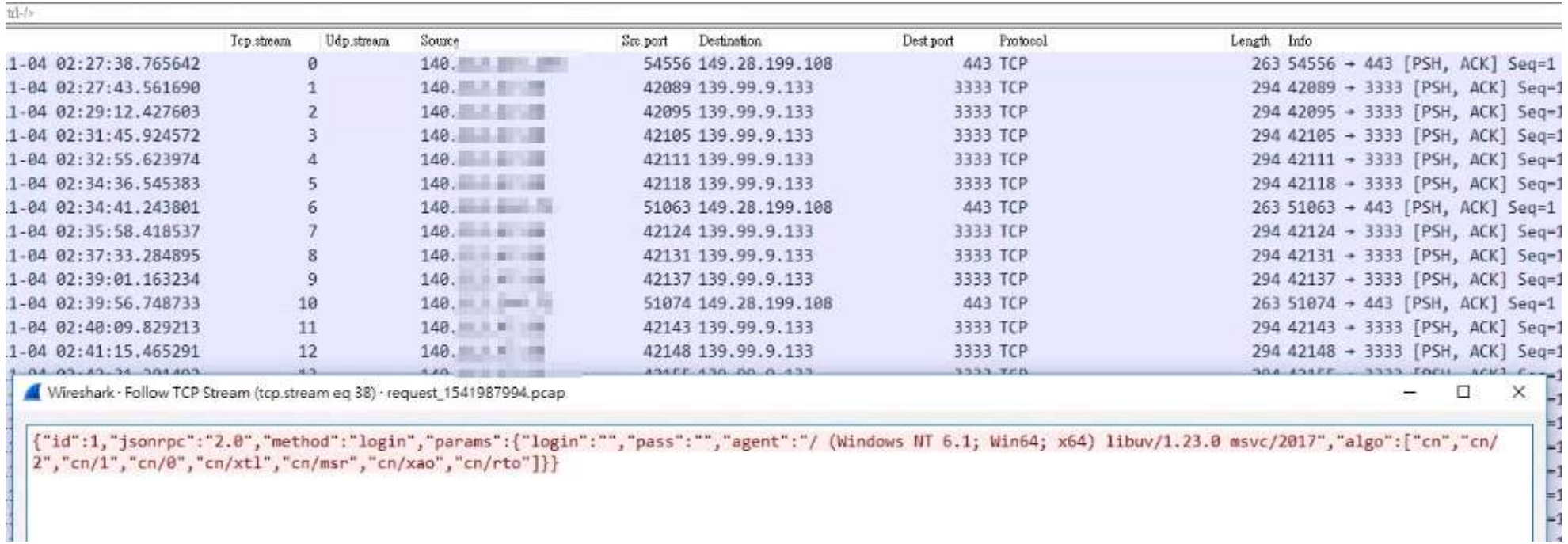
加密貨幣挖礦
(PUA-OTHER Cryptocurrency Miner outbound connection attempt)

PUA-OTHER Cryptocurrency Miner outbound connection attempt，經過查詢大部分封包皆為門羅幣的挖礦事件。



加密貨幣挖礦
(PUA-OTHER Cryptocurrency Miner outbound connection attempt)

經分析之後，可以發現此 IP 為 coinhive 挖礦程式的 domian。

Passive DNS Replication ⓘ

a.deepsecu.com

Date resolved	IP address
2018-11-05	149.28.199.108

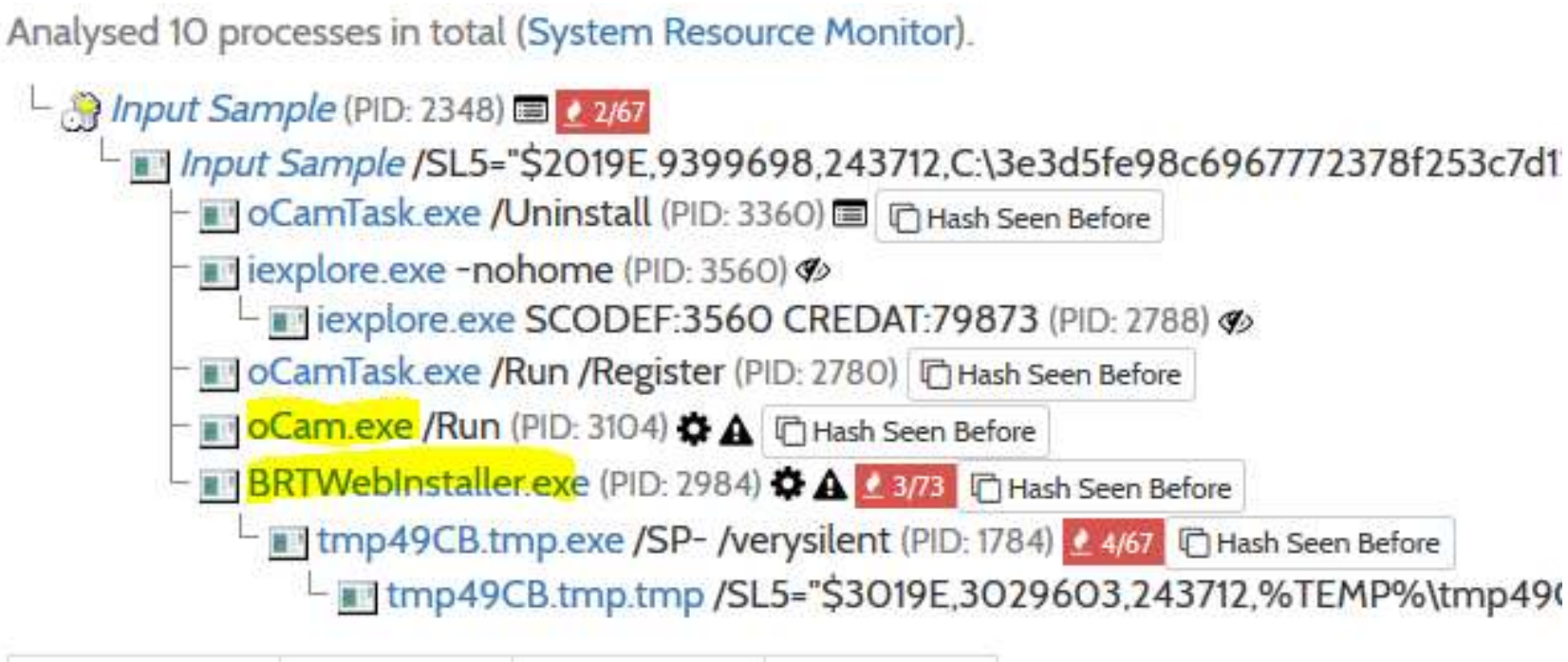
Passive DNS Replication ⓘ

p.deepsecu.com

Date resolved	IP address
2018-10-31	172.104.188.159
2018-06-19	163.44.149.205
2018-06-08	118.27.7.221

加密貨幣挖礦
(PUA-OTHER Cryptocurrency Miner outbound connection attempt)

深入研究封包特徵後，可以發現依然與 oCam 錄影程式相關，其挖礦贊助軟體BRT.exe。



總結

1. 本次事件與先前 ohsoft mining 事件，起因皆為oCam BRT挖礦事件。

2. 建議使用者移除BRTweblnstaller.exe

3. 以及移除BRTSvc，如下圖