

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。

The image shows a Wireshark network traffic capture. The top part is a packet list table with columns for Time, Tcp.stream, Udp.stream, Source, Src.port, Destination, Dest.port, Protocol, Length, and Info. The packets are all TCP connections from source IP 140.203.121.103 to various destinations, mostly 139.99.9.133 and 149.28.199.108, on ports 443 and 3333. The bottom part shows a detailed view of a TCP stream (eq 38) containing a JSONRPC login request for Monero mining.

Time	Tcp.stream	Udp.stream	Source	Src.port	Destination	Dest.port	Protocol	Length	Info
1-04 02:27:38.765642	0	0	140.203.121.103	54556	149.28.199.108	443	TCP	263	54556 → 443 [PSH, ACK] Seq=1
1-04 02:27:43.561690	1	1	140.203.121.103	42089	139.99.9.133	3333	TCP	294	42089 → 3333 [PSH, ACK] Seq=1
1-04 02:29:12.427603	2	2	140.203.121.103	42095	139.99.9.133	3333	TCP	294	42095 → 3333 [PSH, ACK] Seq=1
1-04 02:31:45.924572	3	3	140.203.121.103	42105	139.99.9.133	3333	TCP	294	42105 → 3333 [PSH, ACK] Seq=1
1-04 02:32:55.623974	4	4	140.203.121.103	42111	139.99.9.133	3333	TCP	294	42111 → 3333 [PSH, ACK] Seq=1
1-04 02:34:36.545383	5	5	140.203.121.103	42118	139.99.9.133	3333	TCP	294	42118 → 3333 [PSH, ACK] Seq=1
1-04 02:34:41.243801	6	6	140.203.121.103	51063	149.28.199.108	443	TCP	263	51063 → 443 [PSH, ACK] Seq=1
1-04 02:35:58.418537	7	7	140.203.121.103	42124	139.99.9.133	3333	TCP	294	42124 → 3333 [PSH, ACK] Seq=1
1-04 02:37:33.284895	8	8	140.203.121.103	42131	139.99.9.133	3333	TCP	294	42131 → 3333 [PSH, ACK] Seq=1
1-04 02:39:01.163234	9	9	140.203.121.103	42137	139.99.9.133	3333	TCP	294	42137 → 3333 [PSH, ACK] Seq=1
1-04 02:39:56.748733	10	10	140.203.121.103	51074	149.28.199.108	443	TCP	263	51074 → 443 [PSH, ACK] Seq=1
1-04 02:40:09.829213	11	11	140.203.121.103	42143	139.99.9.133	3333	TCP	294	42143 → 3333 [PSH, ACK] Seq=1
1-04 02:41:15.465291	12	12	140.203.121.103	42148	139.99.9.133	3333	TCP	294	42148 → 3333 [PSH, ACK] Seq=1

```
Wireshark - Follow TCP Stream (tcp.stream eq 38) - request_1541987994.pcap  
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"","pass":"","agent":"/ (Windows NT 6.1; Win64; x64) libuv/1.23.0 msvc/2017","algo":["cn","cn/2","cn/1","cn/0","cn/xt1","cn/msr","cn/xao","cn/rto"]}}
```

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

Passive DNS Replication ⓘ

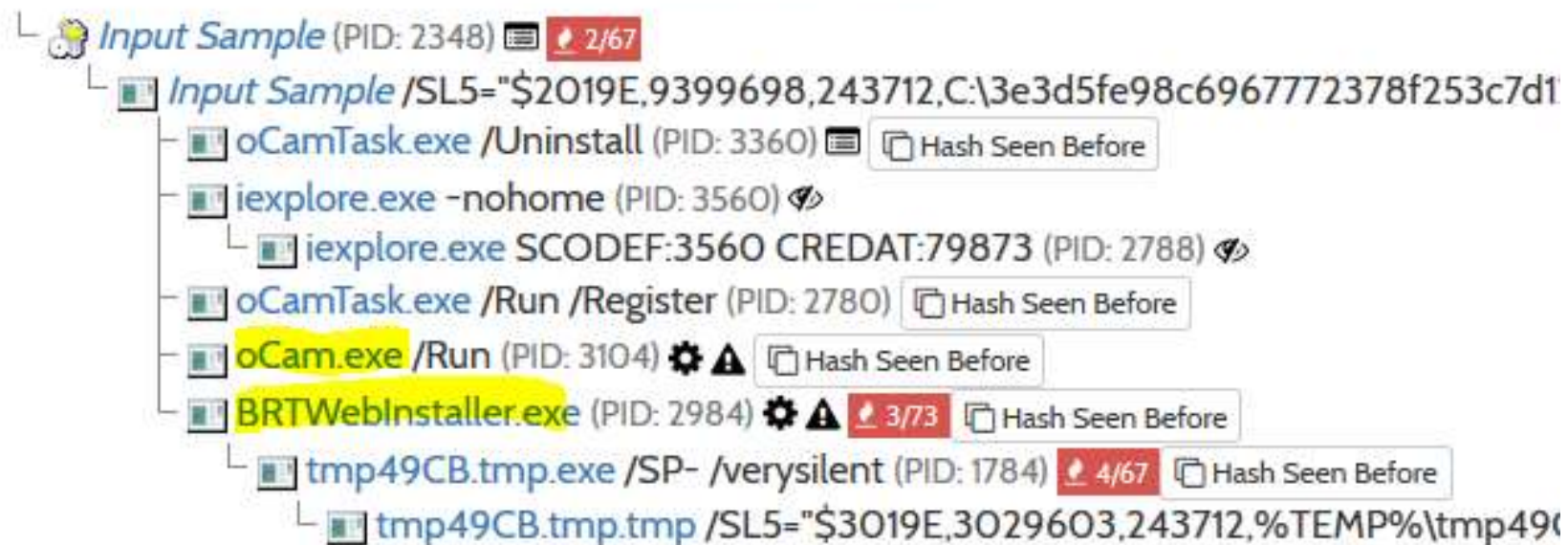
Date resolved	a.deepsecu.com	IP address
2018-11-05		149.28.199.108

Passive DNS Replication ⓘ

Date resolved	p.deepsecu.com	IP address
2018-10-31		172.104.188.159
2018-06-19		163.44.149.205
2018-06-08		118.27.7.221

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。

Analysed 10 processes in total (System Resource Monitor).



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BRTwebInstaller.exe
3. 以及移除BRTSvc，如下圖

