ASOC
事件分析

台大ASOC 11/28

北區ASOC- 11月份開單統計

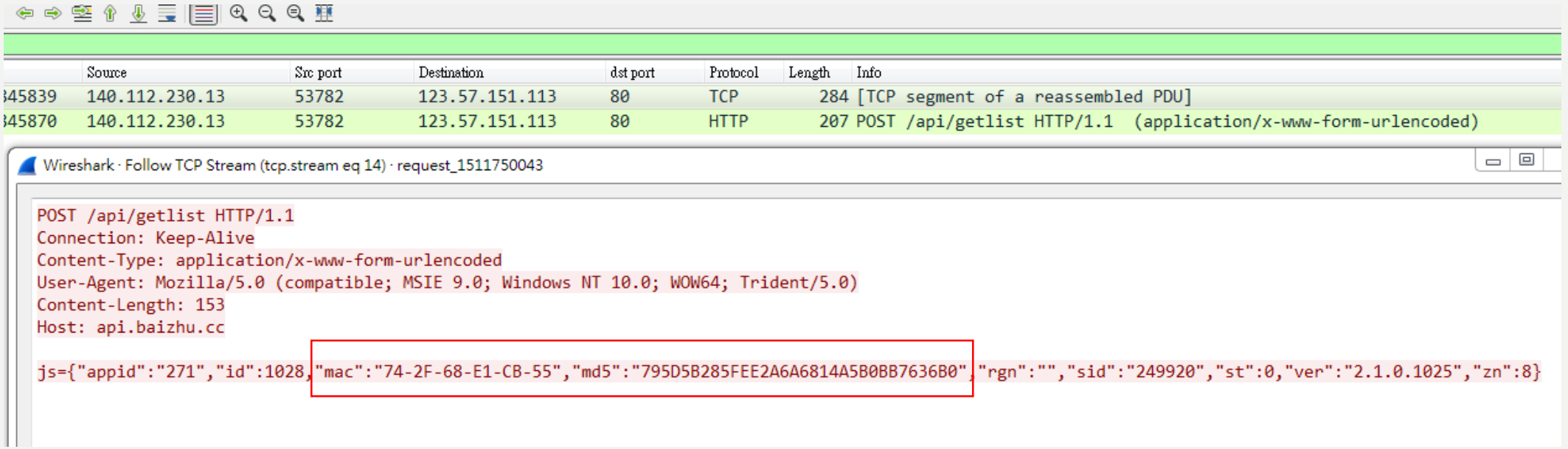
- 北區ASOC統計11月份開單
  前三名分別為
  1. MALWARE-CNC Win.Trojan.Donvibs variant outbound connection attempt
  2. Mining Server
  3. MALWARE-CNC Win.Trojan.Quimonk variant outbound connection detected

11月 - 北區ASOC開單統計	統計
MALWARE-CNC Win.Trojan.Donvibs variant outbound connection attempt	1266
Mining Server	292
MALWARE-CNC Win.Trojan.Quimonk variant outbound connection detected	229
MALWARE-CNC Andr.Trojan.Congur variant outbound connection detected	172
MALWARE-CNC Win.Trojan.Agent outbound connection	160
MALWARE-CNC Win.Trojan.Sality variant outbound connection	91

MALWARE-CNC WIN.TROJAN.QUIMONK VARIANT OUTBOUND CONNECTION DETECTED

- ASOC針對第三名事件進行分析

  發現此事件會將 MAC Address 及 MD5 資訊傳送至 api.baizhu.cc (中國網站)。



	Source	Src port	Destination	dst port	Protocol	Length	Info
345839	140.112.230.13	53782	123.57.151.113	80	TCP	284	[TCP segment of a reassembled PDU]
345870	140.112.230.13	53782	123.57.151.113	80	HTTP	207	POST /api/getlist HTTP/1.1 (application/x-www-form-urlencoded)

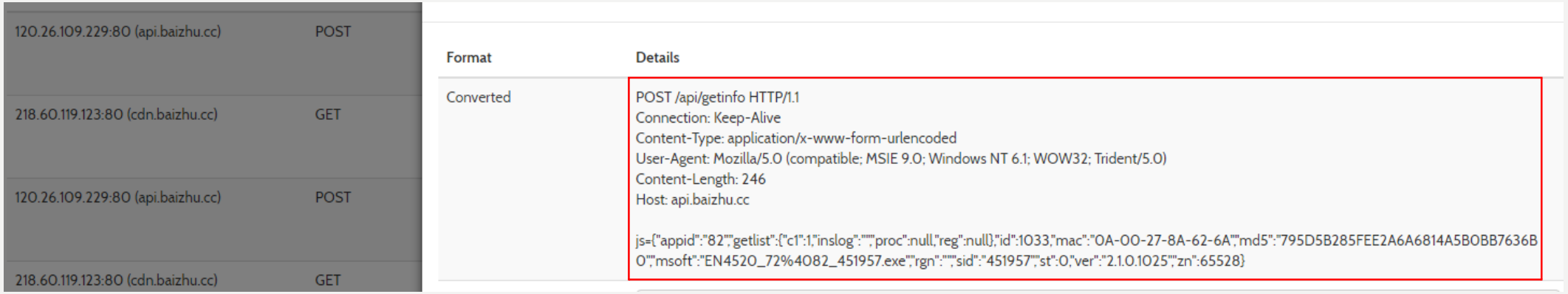
Wireshark · Follow TCP Stream (tcp.stream eq 14) · request_1511750043

```
POST /api/getlist HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; WOW64; Trident/5.0)
Content-Length: 153
Host: api.baizhu.cc

js={"appid":"271","id":1028,"mac":"74-2F-68-E1-CB-55","md5":"795D5B285FEE2A6A6814A5B0BB7636B0","rgn":"","sid":"249920","st":0,"ver":"2.1.0.1025","zn":8}
```

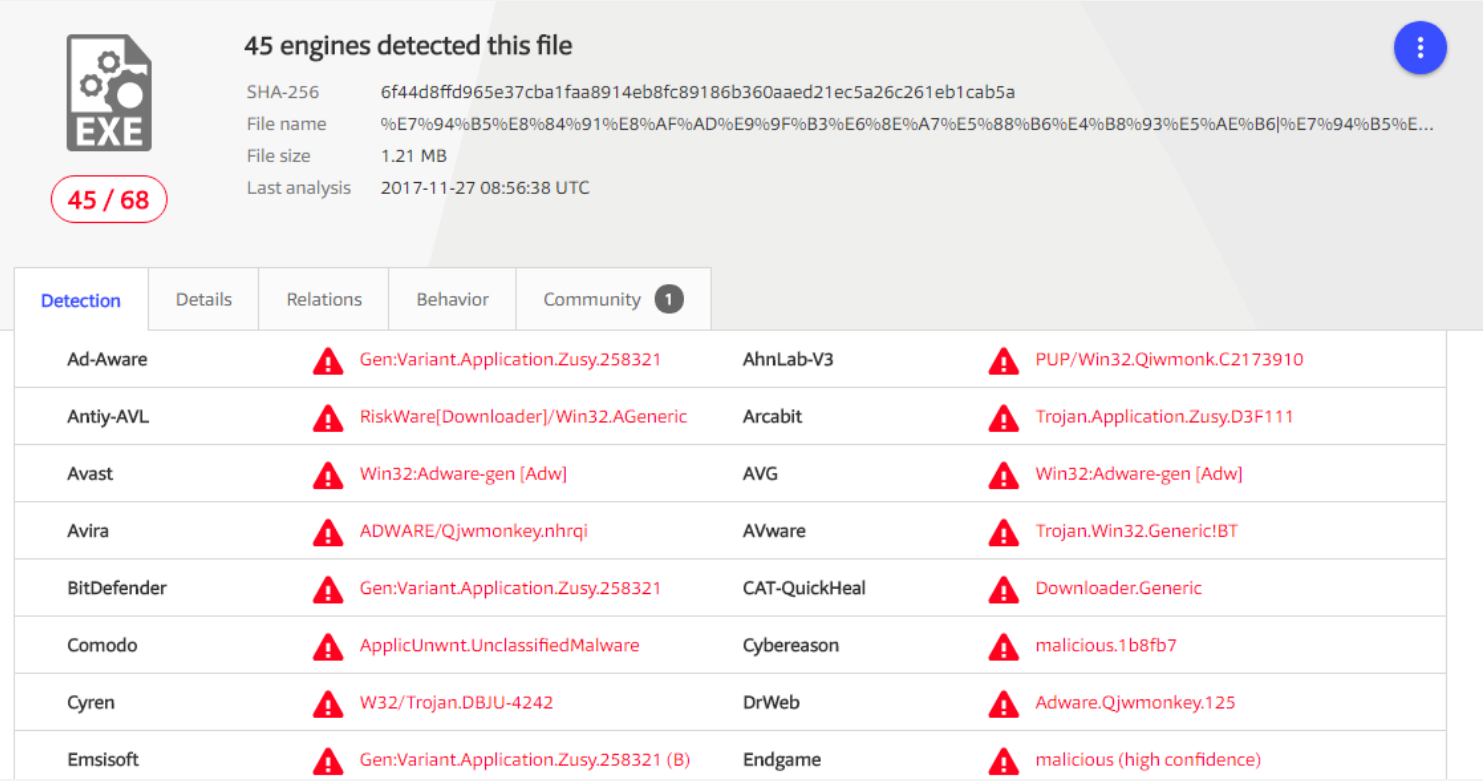
MALWARE-CNC WIN.TROJAN.QUIMONK VARIANT OUTBOUND CONNECTION DETECTED

- 透過封包特徵進行比對，發現此行為早已被關注。



MALWARE-CNC WIN.TROJAN.QUIMONK VARIANT OUTBOUND CONNECTION DETECTED

- 從惡意軟體分析網站Virustotal 能看出此程式，已遭各類防毒軟體認定為惡意程式



MALWARE-CNC WIN.TROJAN.QUIMONK VARIANT OUTBOUND CONNECTION DETECTED

- 其惡意程式以下載器的形式，透過下載器替使用者載入含有惡意軟體的程式。

MALWARE-CNC WIN.TROJAN.QUIMONK VARIANT OUTBOUND CONNECTION DETECTED

- 建議

  因此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