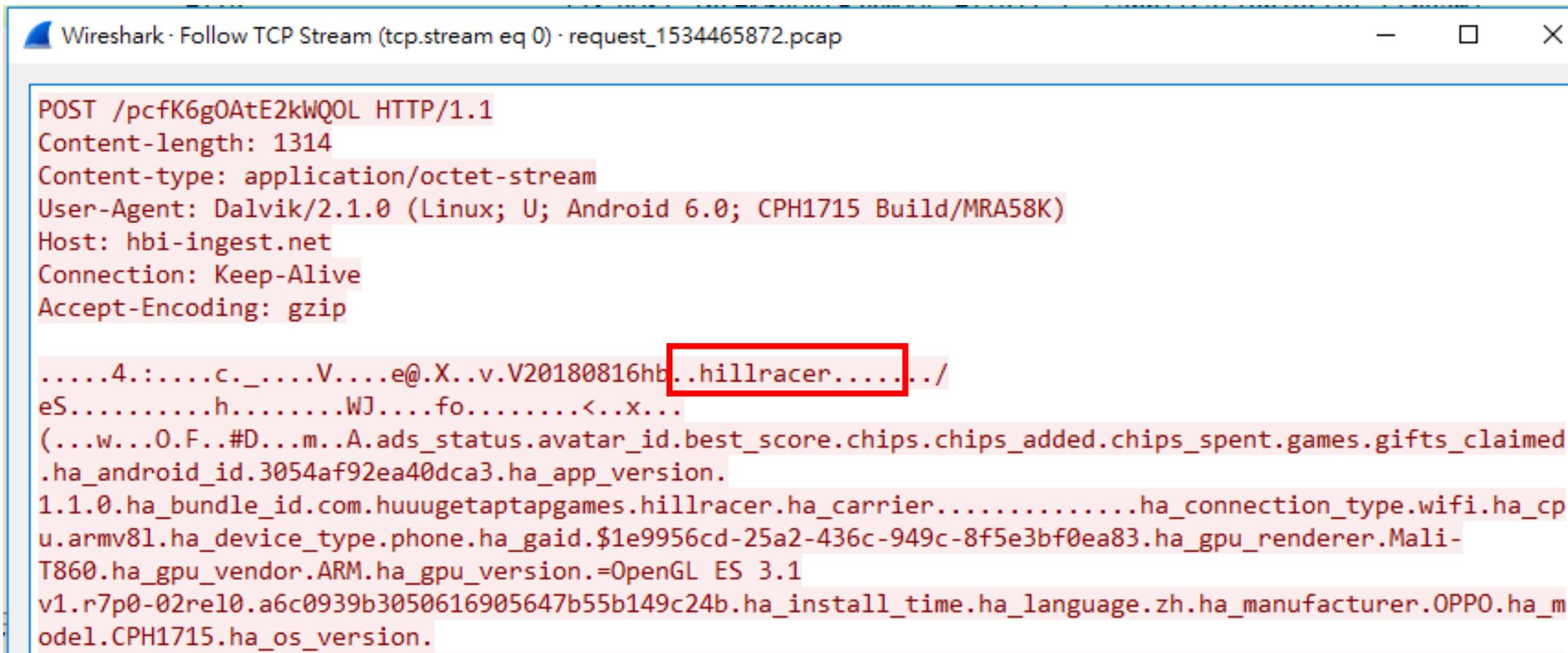


Trojan.Banker報告

Trojan.Banker報告

開始了解原因，以及解決辦法，下圖為該事件的封包。並找到關鍵字 **Hill Racer**



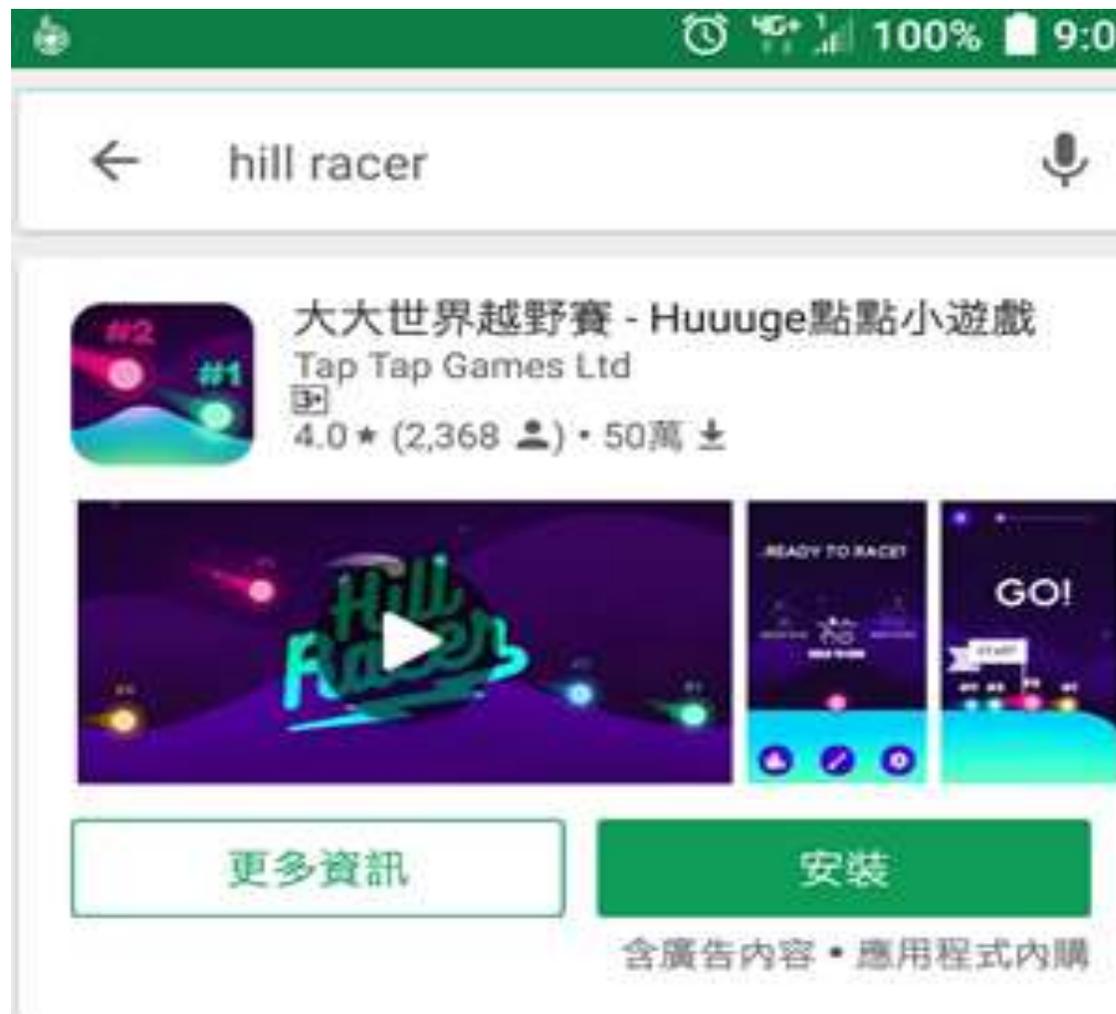
```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · request_1534465872.pcap

POST /pcfK6g0AtE2kWQ0L HTTP/1.1
Content-length: 1314
Content-type: application/octet-stream
User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; CPH1715 Build/MRA58K)
Host: hbi-ingest.net
Connection: Keep-Alive
Accept-Encoding: gzip

.....4.:.....c._.....V.....e@.X..v.V20180816hb..hillracer...../
eS.....h.....WJ....fo.....<..x...
(...w...O.F..#D...m..A.ads_status.avatar_id.best_score.chips.chips_added.chips_spent.games.gifts_claimed
.ha_android_id.3054af92ea40dca3.ha_app_version.
1.1.0.ha_bundle_id.com.huuugetaptapgames.hillracer.ha_carrier.....ha_connection_type.wifi.ha_cp
u.armv81.ha_device_type.phone.ha_gaid.$1e9956cd-25a2-436c-949c-8f5e3bf0ea83.ha_gpu_renderer.Mali-
T860.ha_gpu_vendor.ARM.ha_gpu_version.=OpenGL ES 3.1
v1.r7p0-02rel0.a6c0939b3050616905647b55b149c24b.ha_install_time.ha_language.zh.ha_manufacturer.OPPO.ha_m
odel.CPH1715.ha_os_version.
```

Trojan.Banker報告

上網搜尋後發現為APP遊戲



Trojan.Banker報告

ASOC隨即分析該APP的連線行為，研究連線的目標，和封包內容

The screenshot displays a network analysis tool interface with three main sections:

- Top Section (Traffic Log):** A table listing network traffic. The selected entry (No. 21) shows a connection from source 140.112.3.62 to destination 140.112.3.62 on port 80.
- Middle Section (App Interface):** A mobile application window titled "TRACK 1" with a progress indicator at 17. It features a "HOLD TO LAND" button and a "#4" label. The interface is dark-themed with purple and yellow accents.
- Right Section (Packet Details):** A list of network packets. The selected packet (No. 21) is an application/octet-stream with a length of 66 bytes. The details below show the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.
- Bottom Section (Hex Dump):** A hex dump of the captured data, showing the first 66 bytes of the frame.

Hex Dump Data:

```

0000  00 26 0a 27 1c 80 10 78 d2 c9 59 6f 08 00 45 00  .&...x..Yo..E.
0010  00 34 06 33 40 00 80 06 b6 f9 8c 70 03 3e 34 36  .4.3@.....p.>46
0020  79 b3 82 a9 00 50 cf e8 41 bb 00 00 00 00 02  y....P...A.....
0030  20 00 7c e1 00 02 04 05 b4 01 03 03 02 01 01  .|.....
0040  04 02  ..
  
```

Trojan.Banker報告

ASOC發現遊戲進行時會自動連線到 **hbi-ingest[.]net**，透過各網站檢測後，顯示此網站不安全

General Information

Date:	09.04.2018
Duration:	0h 3m 7s
Sample URL:	http://hbi-ingest.net/evt
Cookbook:	browseurl.jbs
Icon:	No Icon
Filetype:	unknown

Show File Information

Detection

CLEAN

- Found **1** malicious signature
- Contacts **3** domains/IPs
- Launches **3** processes
- Drops **29** files

Signature Overview

Networking	7
Malware Analysis System Evasion	1
Hooking and other Techniques for Hiding and Prot...	1

Show Signature Information

Classification

建議

- 1.建議同學移除該APP遊戲，並且進行手機掃毒。
- 2.如不能強制要求同學移除，會建議阻擋下列IP。

52.4.148.49

52.0.41.251

52.54.121.179