

Snowfox 事件分析

林宜進

事件介紹

- ▶ 資安事件全名: MALWARE-CNC Andr.Tool.Snowfox
Androidbauts/snowfox outbound connection
- ▶ 10月份此事件總共觸發317筆(不分區網中心)
- ▶ Androidbauts是屬於一種android上的廣告軟體(adware), 但是它會回傳裝置內部資訊(例如:IMSI、IMEI、GPS位置)給CNC主機


備註:

國際移動設備識別碼 (International Mobile Equipment Identity , IMEI)

國際移動用戶識別碼 (International Mobile Subscriber Identity , IMSI)

相關檔案掃描結果

- ▶ 因為有問題的軟體已經下架，目前找到相關紀錄如下圖




SHA256: 1b97ed9b1cf0785e2595da480339af7338fb0eb4539fe362b9997301a10d6e46

File name: jjeke-141531-2015092.apk

Detection ratio: 15 / 53

Analysis date: 2015-12-30 05:33:43 UTC (1 year, 11 months ago)



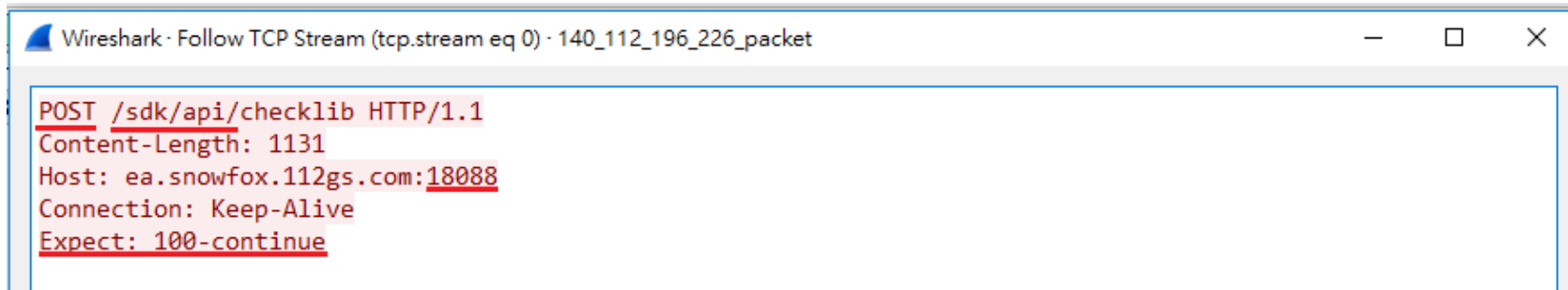
Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
Ad-Aware	Android.Adware.SnowFox.A	20151224
AhnLab-V3	Android-PUP/Snofox.11cd4	20151229
Arcabit	Android.Adware.SnowFox.A	20151230
AVG	Android/Deng.QQE	20151230
BitDefender	Android.Adware.SnowFox.A	20151230
DrWeb	Android.Backdoor.176.origin	20151229
Emsisoft	Android.Adware.SnowFox.A (B)	20151230
ESET-NOD32	a variant of Android/Xinyinhe.N potentially unwanted	20151230
F-Secure	Android.Adware.SnowFox	20151230

觸發規則(都要符合才會觸發)

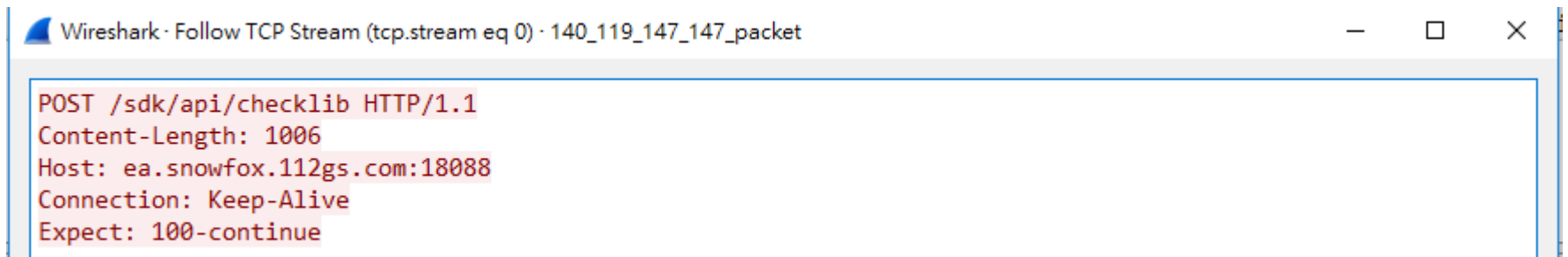
1. 內對外連線，目標埠(dst port)為8088、18001、18088其中之一
2. 封包內容有以下特徵
 - ① POST
 - ② /sdk/api/
 - ③ Expect: 100-continue
3. 封包內容不包括此特徵: User-Agent

問題封包範例



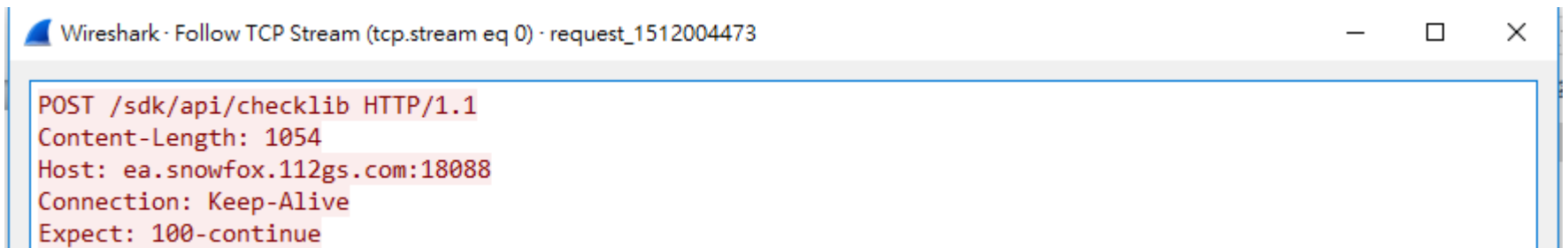
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 140_112_196_226_packet

```
POST /sdk/api/checklib HTTP/1.1
Content-Length: 1131
Host: ea.snowfox.112gs.com:18088
Connection: Keep-Alive
Expect: 100-continue
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · 140_119_147_147_packet

```
POST /sdk/api/checklib HTTP/1.1
Content-Length: 1006
Host: ea.snowfox.112gs.com:18088
Connection: Keep-Alive
Expect: 100-continue
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · request_1512004473

```
POST /sdk/api/checklib HTTP/1.1
Content-Length: 1054
Host: ea.snowfox.112gs.com:18088
Connection: Keep-Alive
Expect: 100-continue
```

連線網址分析-1

- ▶ 網址: ea.snowfox.112gs.com
- ▶ IP: 35.162.109.206
- ▶ 查詢此IP的位置屬於美國
- ▶ 把該網址丟入VirusTotal，沒發現任何問題

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2017-11-1)

IP Address	Country	Region	City
35.162.109.206	United States 🇺🇸	Oregon	Portland
ISP	Organization	Latitude	Longitude
Amazon.com Inc.	Not Available	45.5234	-122.6762



URL: <http://ea.snowfox.112gs.com/>

Detection ratio: 0 / 66

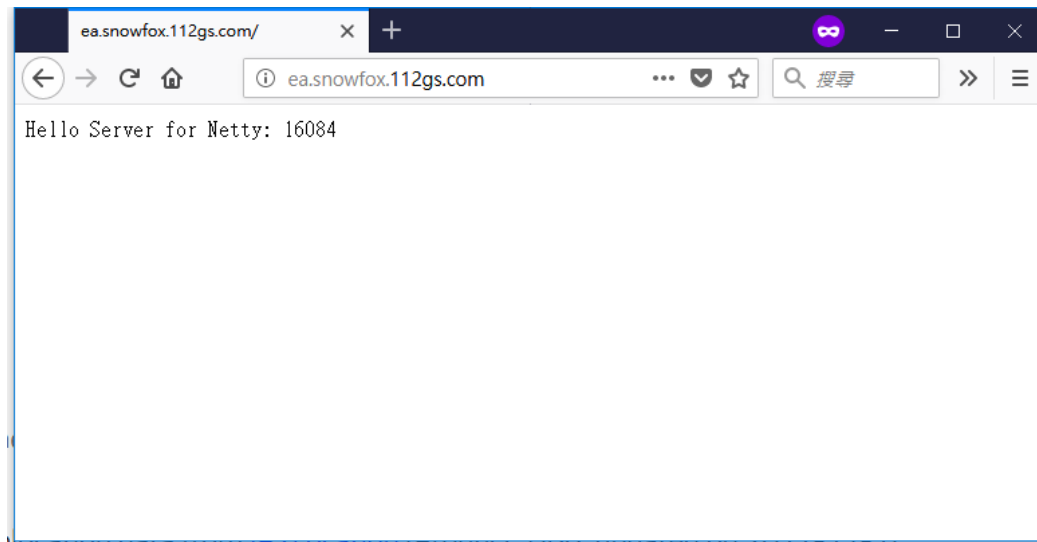
Analysis date: 2017-11-30 06:23:35 UTC (0 minutes ago)

Analysis Additional information Comments Votes

URL Scanner	Result
ADMINUSLabs	Clean site
AegisLab WebGuard	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira (no cloud)	Clean site
Baidu-International	Clean site
BitDefender	Clean site
Blueliv	Clean site
C-SIRT	Clean site

連線網址分析-2

- ▶ 用虛擬主機去連線，得到的畫面如左下圖
- ▶ 只有這行訊息: **Hello Server for Netty: 16081**



連線網址分析-3

- ▶ 用wireshark側錄封包結果如下圖(正常連線的封包)

The image displays a Wireshark capture of an HTTP connection. The main packet list shows a sequence of packets from source 192.168.1.54 to destination 35.162.109.206. Packet 5 is the GET request, and packet 6 is the 200 OK response. The packet details pane for packet 6 shows the response structure: HTTP/1.1 200 OK, Server: nginx, Date: Thu, 30 Nov 2017 06:50:39 GMT, Content-Type: text/plain; charset=UTF-8, Content-Length: 29, and Connection: close. The raw data pane shows the hex and ASCII representation of the response body, which is "Hello Server for Netty: 16082".

No.	Time	Source	src.port	Destination	dst.port	Protocol	Length	Info
1	0.000000	192.168.1.54	6350	35.162.109.206	80	TCP	66	6350 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 ...
2	0.162481	35.162.109.206	80	192.168.1.54	6350	TCP	66	80 → 6350 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1...
3	0.162587	192.168.1.54	6350	35.162.109.206	80	TCP	54	6350 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.162800	192.168.1.54	6350	35.162.109.206	80	HTTP	431	GET / HTTP/1.1
5	0.325378	35.162.109.206	80	192.168.1.54	6350	TCP	60	80 → 6350 [ACK] Seq=1 Ack=378 Win=28032 Len=0
6	0.325402	35.162.109.206	80	192.168.1.54	6350	HTTP	234	HTTP/1.1 200 OK (text/plain)
7	0.325417	35.162.109.206	80	192.168.1.54	6350	TCP	60	80 → 6350 [FIN, ACK] Seq=181 Ack=378 Win=28032 Len=0
8	0.325467	192.168.1.54	6350	35.162.109.206	80	TCP	54	6350 → 80 [ACK] Seq=378 Ack=182 Win=65280 Len=0
9	0.325743	192.168.1.54	6350	35.162.109.206	80	TCP	54	6350 → 80 [FIN, ACK] Seq=378 Ack=182 Win=65280 Len=0
10	0.487451	35.162.109.206	80	192.168.1.54	6350	TCP	60	80 → 6350 [ACK] Seq=182 Ack=379 Win=28032 Len=0

```
GET / HTTP/1.1
Host: ea.snowfox.112gs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101
Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 30 Nov 2017 06:50:39 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 29
Connection: close

Hello Server for Netty: 16082
```


結論

- ▶ 目前**Google play**上大部分的軟體都是沒問題，有問題的軟體都下架了
- ▶ 如果還有使用上的疑慮，可以安裝免費的防毒軟體
- ▶ 該主機似乎被當成跳板
- ▶ 請使用者不要去來路不明的網站下載**apk**檔安裝

參考來源

- ▶ <https://www.bitsighttech.com/blog/androidbauts-advertising-with-a-bit-more-than-expected>
- ▶ <https://dotblogs.com.tw/marcus116/archive/2011/05/29/26428.aspx>
- ▶ <https://www.virustotal.com/en/url/cf5a4a1e76769e4d52c48fa8bda5fa5ab098d581b1b543860024a62a1a5d56a3/analysis/1512023015/>
- ▶ <https://www.virustotal.com/en/file/1b97ed9b1cf0785e2595da480339af7338fb0eb4539fe362b9997301a10d6e46/analysis/1451453623/>