

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

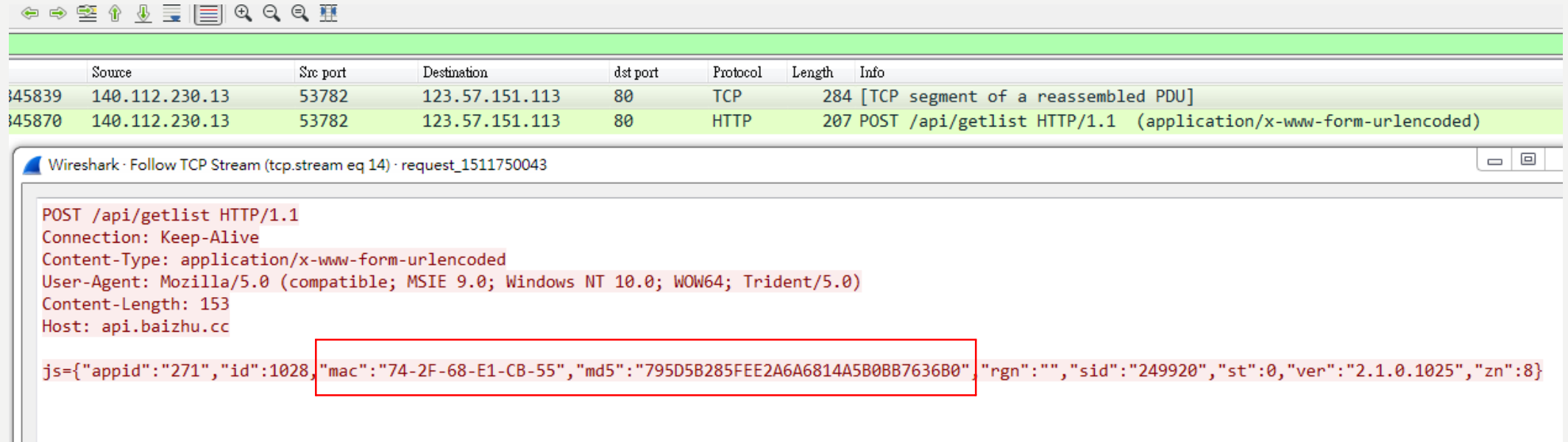
前三名分別為

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)。



The image shows a Wireshark network traffic analysis. The top part is a packet list table with columns: Source, Src port, Destination, dst port, Protocol, Length, and Info. Two packets are highlighted in green:

	Source	Src port	Destination	dst port	Protocol	Length	Info
145839	140.112.230.13	53782	123.57.151.113	80	TCP	284	[TCP segment of a reassembled PDU]
145870	140.112.230.13	53782	123.57.151.113	80	HTTP	207	POST /api/getlist HTTP/1.1 (application/x-www-form-urlencoded)

Below the table is a detailed view of the selected HTTP packet (request_1511750043). The content is as follows:

```
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}
```

The JSON payload is highlighted with a red box, showing the MAC address and MD5 hash being transmitted to the server.

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。

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

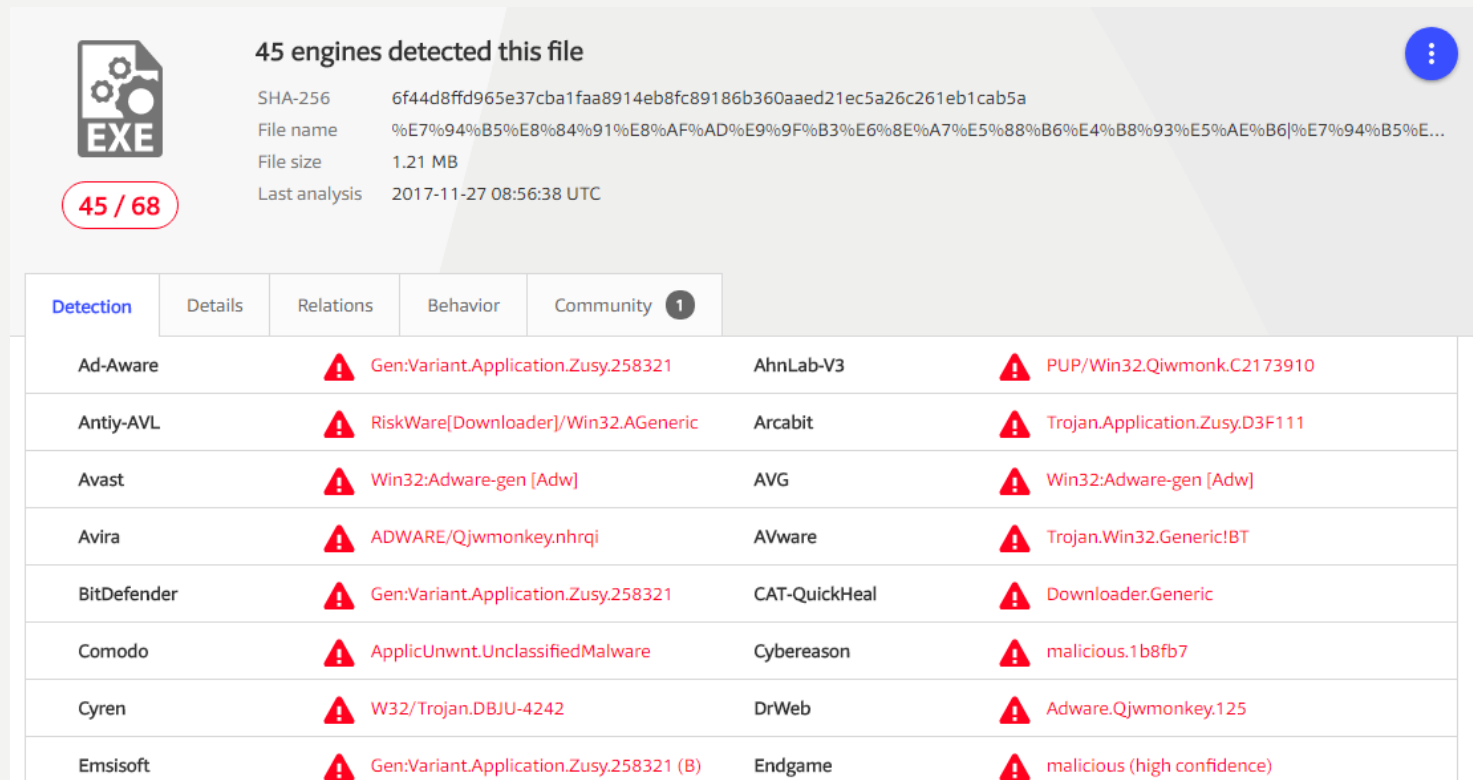
```
POST /api/getlist HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 10.0; WOW64; Trident/5.0)
Content-Length: 153
Host: api.baizhu.cc

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}
```

Format	Details
Converted	POST /api/getinfo HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW32; Trident/5.0) Content-Length: 246 Host: api.baizhu.cc js={"appid":"82","getlist":{"c1":"inslog":"","proc":null,"reg":null,"id":1033,"mac":"0A-00-27-8A-62-6A","md5":"795D5B285FEE2A6A6814A5B0BB7636B0","msoft":"EN4520_72%4082_451957.exe","rgn":"","sid":"451957","st":0,"ver":"2.1.0.1025","zn":65528}}

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



The screenshot shows the VirusTotal analysis page for a file. The file is identified as an EXE and has been detected by 45 out of 68 engines. The analysis details include the SHA-256 hash, file name, file size (1.21 MB), and the last analysis date (2017-11-27 08:56:38 UTC). The detection results are displayed in a table with columns for engine name, detection name, and detection status.

Detection	Details	Relations	Behavior	Community
Ad-Aware	Gen:Variant.Application.Zusy.258321	AhnLab-V3	PUP/Win32.Qjwmonk.C2173910	
Antiy-AVL	RiskWare[Downloader]/Win32.AGeneric	Arcabit	Trojan.Application.Zusy.D3F111	
Avast	Win32:Adware-gen [Adw]	AVG	Win32:Adware-gen [Adw]	
Avira	ADWARE/Qjwmonkey.nhrqi	AVware	Trojan.Win32.Generic!BT	
BitDefender	Gen:Variant.Application.Zusy.258321	CAT-QuickHeal	Downloader.Generic	
Comodo	ApplicUnwnt.UnclassifiedMalware	Cybereason	malicious.1b8fb7	
Cyren	W32/Trojan.DBJU-4242	DrWeb	Adware.Qjwmonkey.125	
Emsisoft	Gen:Variant.Application.Zusy.258321 (B)	Endgame	malicious (high confidence)	

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。

Signature Info ⓘ

Signature Verification

✔ Signed file, valid signature

File Version Information

Copyright	Copyright (C) 2017
Product	智能下載器.exe
Description	智能下載器
Original Name	智能下載器.exe
Internal Name	智能下載器.exe
File Version	2.1.0.1025
Date Signed	10:55 AM 10/30/2017

360安全卫士

软件大小: 1588KB
人气指数: 3559
软件语言: 简体中文
软件评级: ★★★★★
安全检测: 360杀毒通过
QQ检测通过
金山毒霸通过

快速安装

软件简介:
360安全卫士是当前功能最强、效果最好、最受用户欢迎的上网必备安全软件。360安全卫士2015拥有查杀木马、清理插件、修复漏洞、电脑体检等多种功能,并独创了“木马防火墙”功能,依靠抢先检测和云端鉴别,网站下载驱动所有应用自取中快速下载软件,它检测的华

惠普HP ENVY 4522 驱动

软件大小: 132MB
人气指数: 8469
软件语言: 简体中文
软件评级: ★★★★★
安全检测: 360杀毒通过
QQ检测通过
金山毒霸通过

快速安装

软件简介:
惠普HPENVY4522多功能一体机驱动下载版本: 36.0发布日期: 2015-05-08适用于: WindowsXP/WindowsVista/Windows7/Windows8/Windows8.1/Wi

热门推荐软件:

- 腾讯视频
海量视频在线观看
立即体验
- 安全套装
安全软件先驱者
立即体验
- QQ浏览器
属于你的浏览器
立即体验
- 爱奇艺
精彩视频在线观看
立即体验

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>