Adware.Taplika事件說明

MALWARE-CNC Win.Adware.Taplika toolbar download attempt

- Taplika是一個瀏覽器綁架軟體，通過下載免費軟體夾帶檔案進行安裝，一旦安裝它將自動新增Search.us.com工具欄，並將您的瀏覽器的首頁和預設搜索引擎更改為Taplika。

- Taplika在您的搜尋結果（Google，Yahoo，Bing）中顯示廣告和贊助連結，並可能會從您的搜尋查詢以及所訪問的網頁以及展示和點擊的廣告中收集搜尋關鍵字。

出處:北區ASOC整理

Adware.Taplika事件說明

MALWARE-CNC Win.Adware.Taplika toolbar download attempt

- IPS規則如下：若封包內容包含“php?context=”; “&status=”; “&sesid=”; “&iid=”; “&cd=” 等字串

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Adware.Taplika toolbar download attempt"; flow:to_server,established;
content:"php?context="; fast_pattern:only; http_uri; content:"&status="; http_uri; content:"&sesid="; http_uri; content:"&iid="; http_uri; content:"&cd="; http_uri
metadata:impact_flag red, policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, service http;
reference:url,virustotal.com/en/file/6a9b041b65d699da4ecb66b2c0a7321e82a81b4aae03f0d7b7382f8d598bc471/analysis/; classtype:trojan-activity; sid:46963; rev:1; )
```

- 觸發封包如下：確認封包內容將會觸發IPS規則。

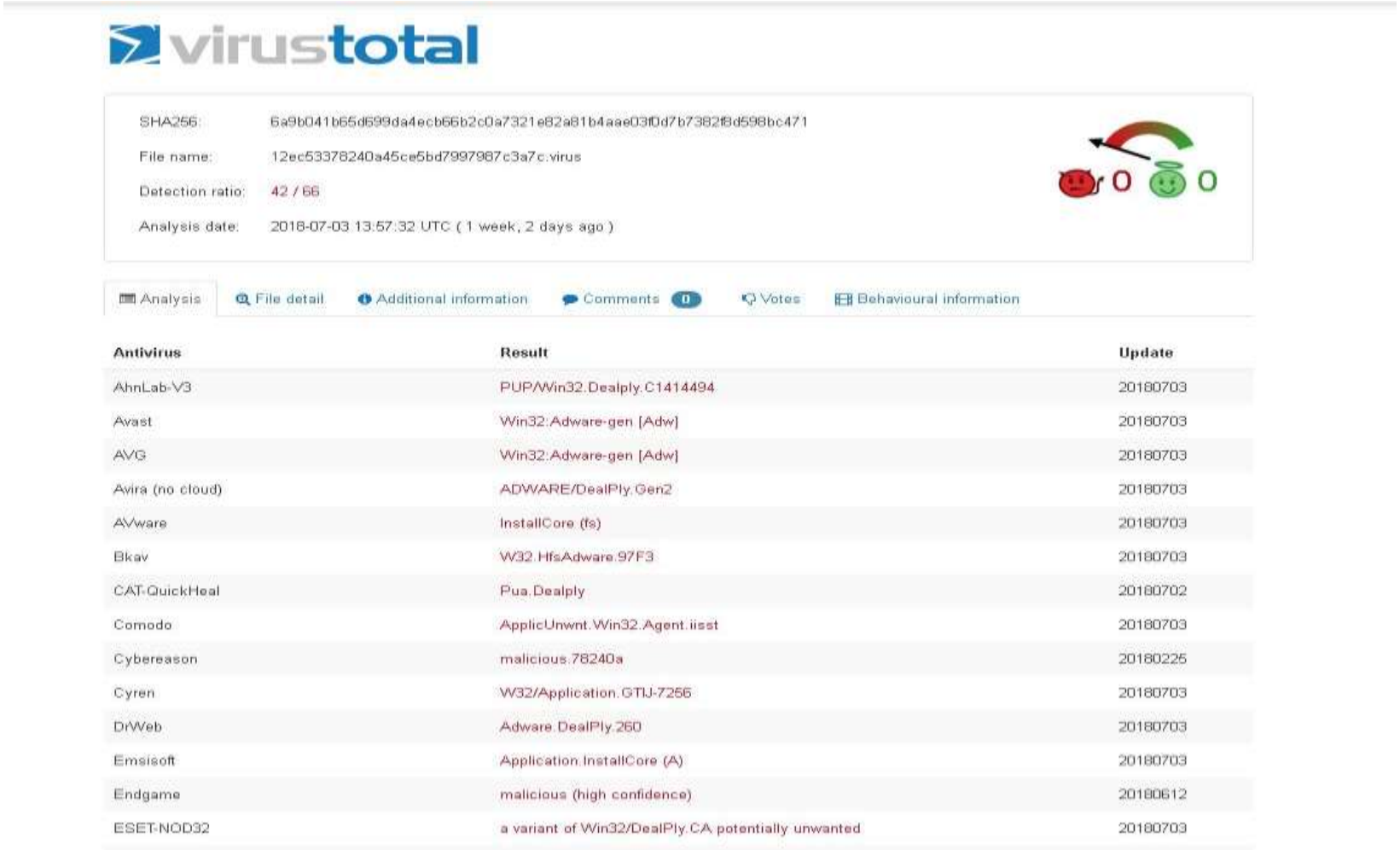
```
GET /p.php?
context=landactivity&status=onclient&sesid=458bce92a6a4dbb9de69b2d96097d867&iid=59d9bc7a6345f
b7bfb26245ac6f92645&cd=2XzuyEtN2Y1L1Qzu0B0C0A0E0CyD0DyC0A0BtCyDyEtBtAzytN0D0Tzu0SzztCtDtN1L2X
zutBtFtCzztFyBtFtDtN1L1CzutCyEtDtAtDyD1V1TtN1L1G1B1V1N2Y1L1Qzu2SyB0F0C0F0FtAtCtBtG0D0AtDtBtGt
CtA0F0FtGyEtC0EyEtGyC0CtAtC0FyC0Ezz0CyBtB0B2QtN1M1F1B2Z1V1N2Y1L1Qzu2StB0BzyzyyD0A0DtDtGzz0E0A
0CtGyByE0EtCtGyEyEyCyCtGtBzz0E0E0C0ByDyC0FzzyC0C2Q&cr=559233275&ir=140305_a&elng=en&a=ir_14_1
2_ie&f=1&cat=web&ulng=en-US%2Cen%3Bq%3D0.9&sid=&csr=0&ipblock=0&1530242358 HTTP/1.1
```

出處:北區ASOC整理

Adware.Taplika事件說明

MALWARE-CNC Win.Adware.Taplika toolbar download attempt

- Virustotal 掃描結果



virustotal

SHA256: 6a9b041b65d699da4ecb66b2c0a7321e82a81b4aae03f0d7b7382f8d598bc471

File name: 12ec53378240a45ce5bd7997987c3a7c.virus

Detection ratio: 42 / 66

Analysis date: 2018-07-03 13:57:32 UTC (1 week, 2 days ago)

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

Antivirus	Result	Update
AhnLab-V3	PUP/Win32.Dealply.C1414494	20180703
Avast	Win32:Adware-gen [Adw]	20180703
AVG	Win32:Adware-gen [Adw]	20180703
Avira (no cloud)	ADWARE/DealPly.Gen2	20180703
AVware	InstallCore (fs)	20180703
Bkav	W32.HfsAdware.97F3	20180703
CAT-QuickHeal	Pua.Dealply	20180702
Comodo	ApplicUnwnt.Win32.Agent.iisst	20180703
Cybereason	malicious.78240a	20180225
Cyren	W32/Application.GTIJ-7256	20180703
DrWeb	Adware.DealPly.260	20180703
Emsisoft	Application.InstallCore (A)	20180703
Endgame	malicious (high confidence)	20180612
ESET-NOD32	a variant of Win32/DealPly.CA potentially unwanted	20180703

出處:北區ASOC整理

Adware.Taplika事件說明

MALWARE-CNC Win.Adware.Taplika toolbar download attempt

- 針對Adware.Taplika首頁綁架軟體可利用下列方式清除
  1.重置瀏覽器首頁及預設搜索引擎
  2.利用**Reason Core Security、AdwCleaner進行廣告軟體的移除**

  AdwCleaner 可以參考GOOGLE搜尋

  https://www.google.com.tw/search?q=AdwCleaner&rlz=1C1SQJL_zh-TWTW785TW786&oq=AdwCleaner&aqs=chrome..69i57.651j0j4&sourceid=chrome&ie=UTF-8

出處:北區ASOC整理