個案分析-

偽裝成文件格式的惡意執行檔事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

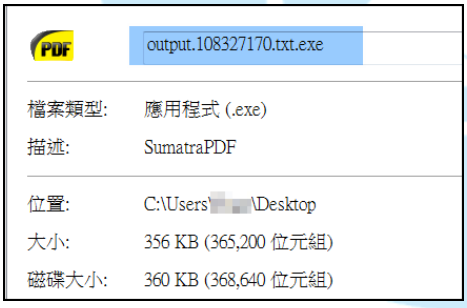
106 年 3 月

I. 事件簡介

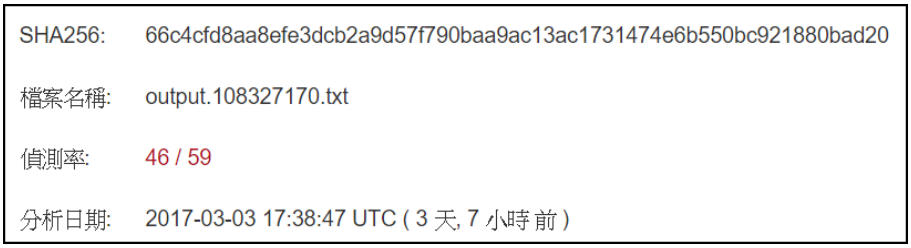
1. 該資安事件為測試網路上取得的惡意程式樣本並觀察其系統及網路行為，分析可能對於電腦主機受到的損害。
2. 該惡意程式為偽裝成文件檔 TXT 的執行程式，名為「output.108327170.txt」的 EXE 檔案。
3. 通常這一類檔案多會依附在 SPAM 垃圾郵件或 APT 郵件中，誘使一般人開啟並遭受感染。
4. 本單位透過使用 Win7(x64)系統的 VM 主機進行隔離測試，並且側錄其網路封包進行分析。

II. 事件檢測

1. 首先將病毒樣本解壓縮後，圖示為 PDF 字樣的 EXE 執行檔，而檔名則是以 TXT 進行偽裝，「output.108327170.txt.exe」，系統預設不會顯示附檔名 EXE，不小心容易誤認為就只是一般的 TXT 文件。



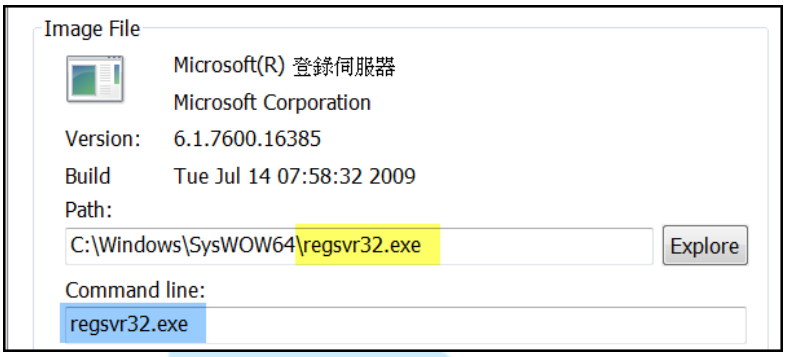
2. 該惡意程式在 Virustotal 上很高的比例 46/59 被偵測為惡意程式。



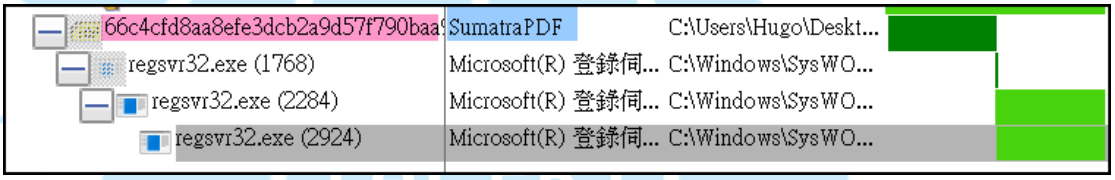
3. 當執行「output.108327170.txt.exe」惡意程式後，該程式原始檔案便會自我移除，讓使用者無法再次取得程式的樣本，如同加密勒索軟體般有自

我銷毀機制。

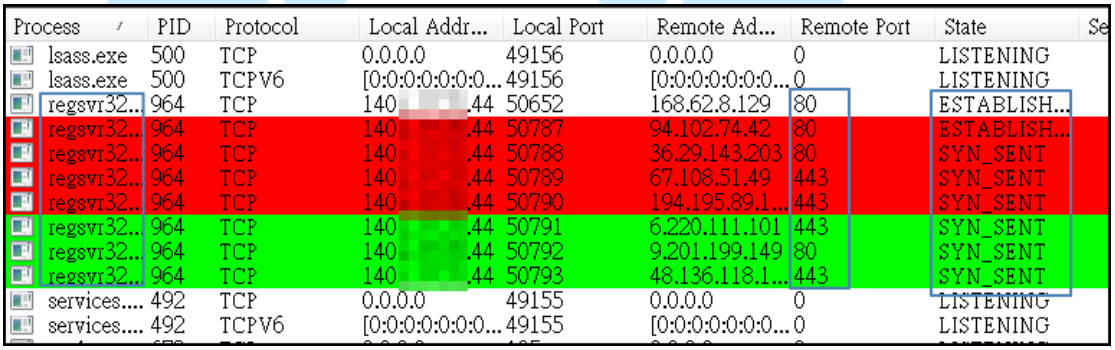
4. 約莫經過一段時間後系統背景開始出現一支名為 regsvr32.exe 程式正在執行，透過 virustotal 檢測並非惡意程式。



5. 檢查 regsvr32.exe 位置位於系統路徑 \SysWOW64\ 中，為系統內建的合法程式，為惡意程式「output.108327170.txt.exe」呼叫執行的子程序。



6. 從連線的 log 紀錄來看，regsvr32.exe 會大量對外部的 port 80 和 443 進行連線，導致系統效能降低。



Process	PID	Protocol	Local Addr...	Local Port	Remote Ad...	Remote Port	State	Se
lsass.exe	500	TCP	0.0.0.0	49156	0.0.0.0	0	LISTENING	
lsass.exe	500	TCPV6	[0:0:0:0:0:0:0...	49156	[0:0:0:0:0:0:0...	0	LISTENING	
regsvr32...	964	TCP	140 .44	50652	168.62.8.129	80	ESTABLISH...	
regsvr32...	964	TCP	140 .44	50787	94.102.74.42	80	ESTABLISH...	
regsvr32...	964	TCP	140 .44	50788	36.29.143.203	80	SYN_SENT	
regsvr32...	964	TCP	140 .44	50789	67.108.51.49	443	SYN_SENT	
regsvr32...	964	TCP	140 .44	50790	194.195.89.1...	443	SYN_SENT	
regsvr32...	964	TCP	140 .44	50791	6.220.111.101	443	SYN_SENT	
regsvr32...	964	TCP	140 .44	50792	9.201.199.149	80	SYN_SENT	
regsvr32...	964	TCP	140 .44	50793	48.136.118.1...	443	SYN_SENT	
services....	492	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING	
services....	492	TCPV6	[0:0:0:0:0:0:0...	49155	[0:0:0:0:0:0:0...	0	LISTENING	

7. 從連線時間的密集度來看，regsvr32.exe 的 HTTP POST 連線 session 間隔不到一秒鐘，並且連線大小大概都在 5KB 左右，算是異常網路流量。

Time	Service	Size	Events	Displaying 1 - 2
2017-Feb-21 11:54:42	IP / TCP / HTTP	5.26 KB	140.[redacted]44 ->	168.62.8.129 49918 -> 80 (http)
2017-Feb-21 11:56:42	IP / TCP / HTTP	5.33 KB	140.[redacted]44 ->	168.62.8.129 50161 -> 80 (http)
2017-Feb-21 11:58:16	IP / TCP / HTTP	3.85 KB	140.[redacted]44 ->	195.90.108.192 50359 -> 80 (http)
2017-Feb-21 11:58:43	IP / TCP / HTTP	5.37 KB	140.[redacted]44 ->	168.62.8.129 50415 -> 80 (http)
2017-Feb-21 12:00:16	IP / TCP / HTTP	3.91 KB	140.[redacted]44 ->	195.90.108.192 50596 -> 80 (http)
2017-Feb-21 12:00:44	IP / TCP / HTTP	5.33 KB	140.[redacted]44 ->	168.62.8.129 50652 -> 80 (http)
2017-Feb-21 12:02:17	IP / TCP / HTTP	3.93 KB	140.[redacted]44 ->	195.90.108.192 50844 -> 80 (http)
2017-Feb-21 12:02:45	IP / TCP / HTTP	5.33 KB	140.[redacted]44 ->	168.62.8.129 50904 -> 80 (http)
2017-Feb-21 12:04:18	IP / TCP / HTTP	3.84 KB	140.[redacted]44 ->	195.90.108.192 51095 -> 80 (http)

8. 先檢測 port 80 的連線封包內容，幾乎都是用 HTTP POST 方式將密文資料傳送出去，嘗試透過 url 和 base64 decoder 對內容解碼，並無法成功還原明文內容。此其中一個連線 IP 168.62.8.129 內容。

2017/2/21 下午 12:06:42 Removed	regsvr32.exe	TCP 140.[redacted]	,44:51416	113.244.251.183:443
2017/2/21 下午 12:06:44 Added	regsvr32.exe	TCP 140.[redacted]	,44:51423	168.62.8.129:80
2017/2/21 下午 12:06:44 Added	regsvr32.exe	TCP 140.[redacted]	,44:51424	158.95.24.223:80
2017/2/21 下午 12:06:44 Added	regsvr32.exe	TCP 140.[redacted]	,44:51425	139.123.19.115:8080

RSA Security Analytics Reconstruction for session ID: 45 (Source 140.[redacted].44 : 52200, Target 168.62.8.129 : 80)
Time 2/21/2017 12:12:48 to 2/21/2017 12:13:50 Calculated Packet Size 5,512 bytes Calculated Payload Size 4,720 bytes

REQUEST

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0
; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center
PC 6.0)
Host: 168.62.8.129
Content-Length: 500
Cache-Control: no-cache

JThFgcIxU7qxdpoQBMb5NEfeTPLbT7DHJVRRt3KXg8KHEjWn8HTwIkrVt5B/Wu+yYS4wjw/kV73hLQug4
foT2eeR+D7wE+57ZV1BzV24J2z7BDLcKdHzBdkD58IwZ0dWaT2BB6/v2Guy/7XaLMZPdm21w/aWWx/cs2
iDWp+Y1OkcWaeX5iHHbjwi5SgF9K1v4o06hzr68xpu8Y86EG6QCDHrGzRfYtMLB17yg2yQ4mMrAFexEbU
VMpkyEK9YTbOx1t5HVKKdvsBLfmO/AC11JAckL9uBQi3rXx1mc3/fSazg8hXGNHt5uoI3an9bbelejkBr
PFuTTB4IZkPz0Ak7/gFqVAC5zPcGhx7pXX+HoN5xgMe0KfNjZz+xcSRNORa5XNkjFCJoin4MvRAZZA88o
SnvUdEnYT+SBRXHkR2i76edY/6jcBVgFrYodyVqdWbG1WMEoi4Ykok9kJCym4oER0ZiK1SayMaCIKeNik
EAF/w1nkosYcA=
```

RESPONSE

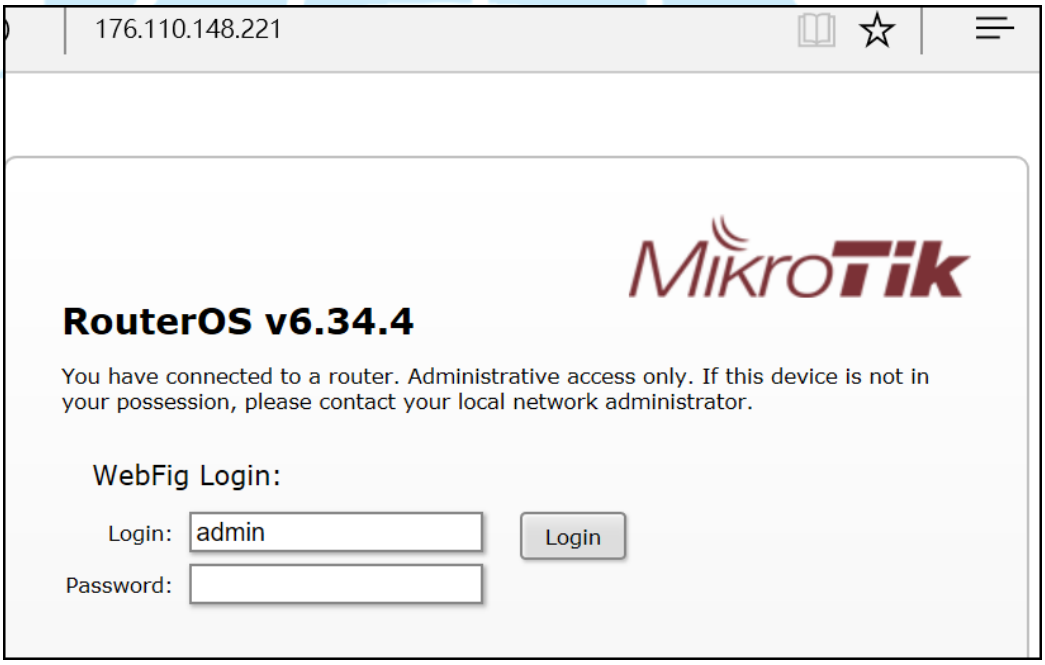
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.0
X-AspNetMvc-Version: 4.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Authorizatio
pe, Accept
Access-Control-Expose-Headers: Authorizati
Date: Tue, 21 Feb 2017 04:12:50 GMT
Content-Length: 2690

<!DOCTYPE html>
<html>
<head>
```

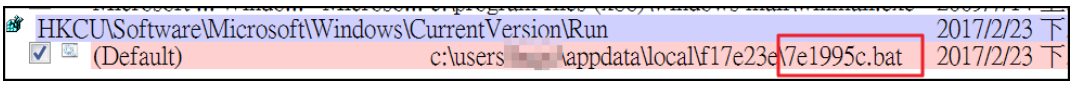
9. 檢測 port 443 其中一個連線封包，regsvr32.exe 連到 IP 217.18.74.60 並且傳輸內文都是加密密文，也無法解密了解其內容，只確定是惡意程式的連線狀態。

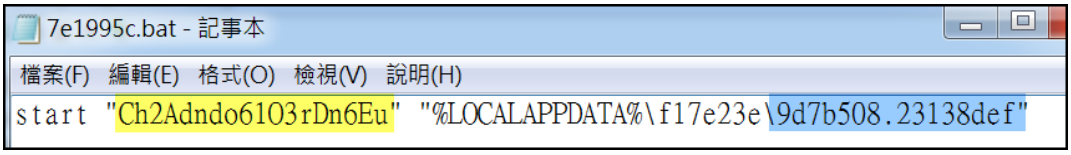
2017/2/21 下午 12:08:07 Removed	regsvr32.exe	TCP 140.[redacted]	44:51602	24.233.219.84:80
2017/2/21 下午 12:08:09 Added	regsvr32.exe	TCP 140.[redacted]	44:51609	63.255.86.35:443
2017/2/21 下午 12:08:09 Added	regsvr32.exe	TCP 140.[redacted]	44:51610	217.18.74.60:443
2017/2/21 下午 12:08:09 Added	regsvr32.exe	TCP 140.[redacted]	44:51611	26.225.207.210:443
2017/2/21 下午 12:08:09 Added	regsvr32.exe	TCP 140.[redacted]	44:51612	119.217.155.29:443

10.從以上連線紀錄來看，連到的 port 80 和 443 的 IP 大多是一般網站或有啟用 WEB 服務主機，研判可能是遭駭客利用的跳板中繼站，用來接收底層殭屍主機回報和下達指令用途。

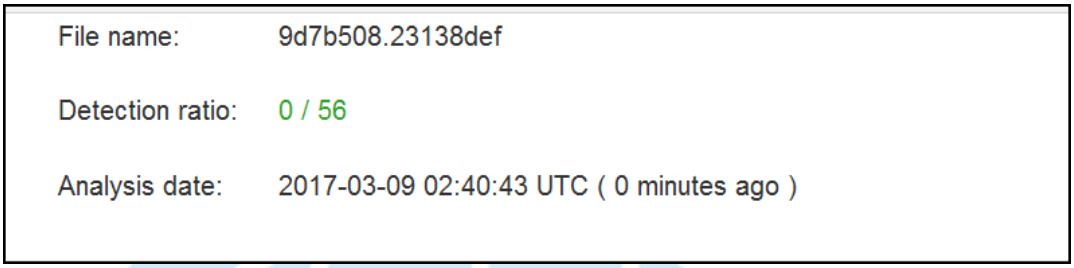


11.檢查開機自動啟動狀態，發現有一個批次檔 「7e1995c.bat」 被寫入啟動程序中，其執行內容為呼叫隱藏資料夾中的惡意程式「9d7b508.23138def」，其中黃色部分為指令視窗標題文字。



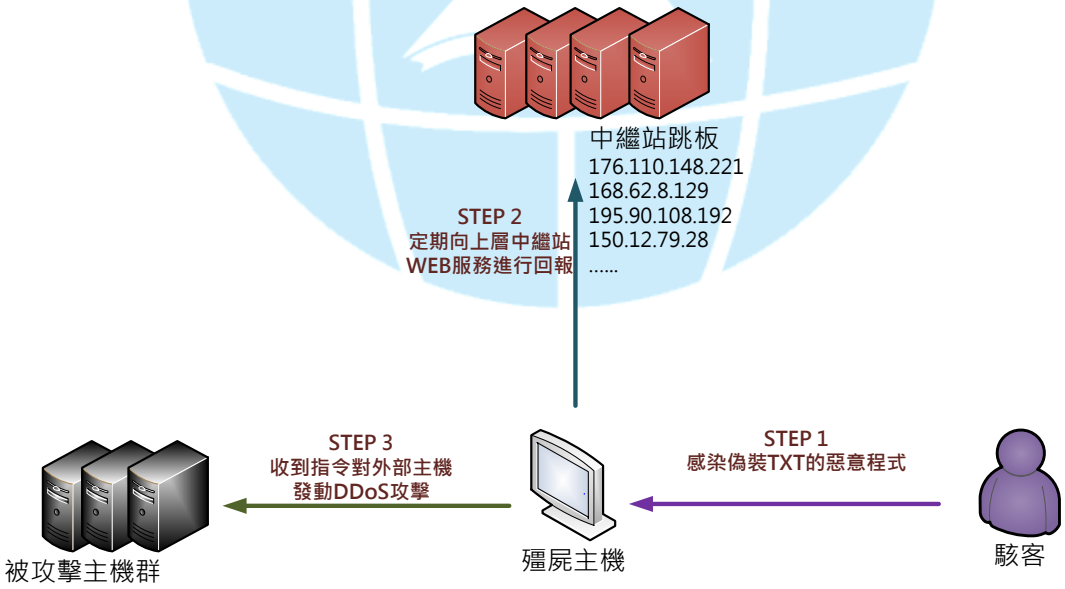


12. 惡意程式「9d7b508.23138def」透過 Virustotal 掃描結果為 0/56，表示該檔案為較為新型的惡意程式或客製化的病毒，通常為 APT 攻擊所用。而該程式啟動後會執行 regsvr32.exe 產生對外惡意的連線。



13. 由於該事件主機沒有接受大量外部 IP 的連入跡象，研判是一般底層殭屍主機而非上層中繼站或 C&C，但可能會接收中繼站或 C&C 指令對外發動攻擊。

III. 網路架構圖



1. 使用者可能從垃圾郵件或釣魚郵件開啟偽裝成 TXT 文件檔的惡意程式。
2. 惡意程式會持續向上層中繼站 port 80 或 443 以加密內容進行回報。

3. 殭屍主機透過定期回報等待 C&C 和中繼站下達攻擊指令。

4. 殭屍主機收到指令後可能會對外部主機進行 DDoS 攻擊。

IV.建議與總結

1. 惡意程式入侵方式可能透過垃圾郵件或釣魚郵件對使用者發動 APT 攻擊，並且附加檔案多為偽造文件的執行檔。
2. 惡意程式執行後會自我刪除，並且感染系統內部檔案並執行系統程式 regsvr32.exe 對外產生網路連線。
3. Regsvr32.exe 會與上層跳板中繼站群 port 80 和 443 進行報到動作，並且等待 C&C 的指令可能對外進行 DDoS 攻擊。
4. 上層中繼站可能都是被駭客入侵有啟用 Web 服務的跳板主機，用來接收來自底層殭屍網路的回報。
5. 惡意程式並會寫入開機啟動執行任務，而執行的惡意程式「9d7b508.23138def」在 Virustotal 上尚無法被偵測出來。
6. 近期許多後門惡意程式經過駭客客製化，規避常用的偵測防毒或檢測，並透過合法程式進行對外連線，故要注意不隨意開啟不明檔案。
7. 因為無法明確移除被感染的檔案，建議使用者將重要資料備份並且重新安裝系統，確保能將惡意程式完全移除。