

InfoSteal 竊聽程式攻擊事件 分析報告

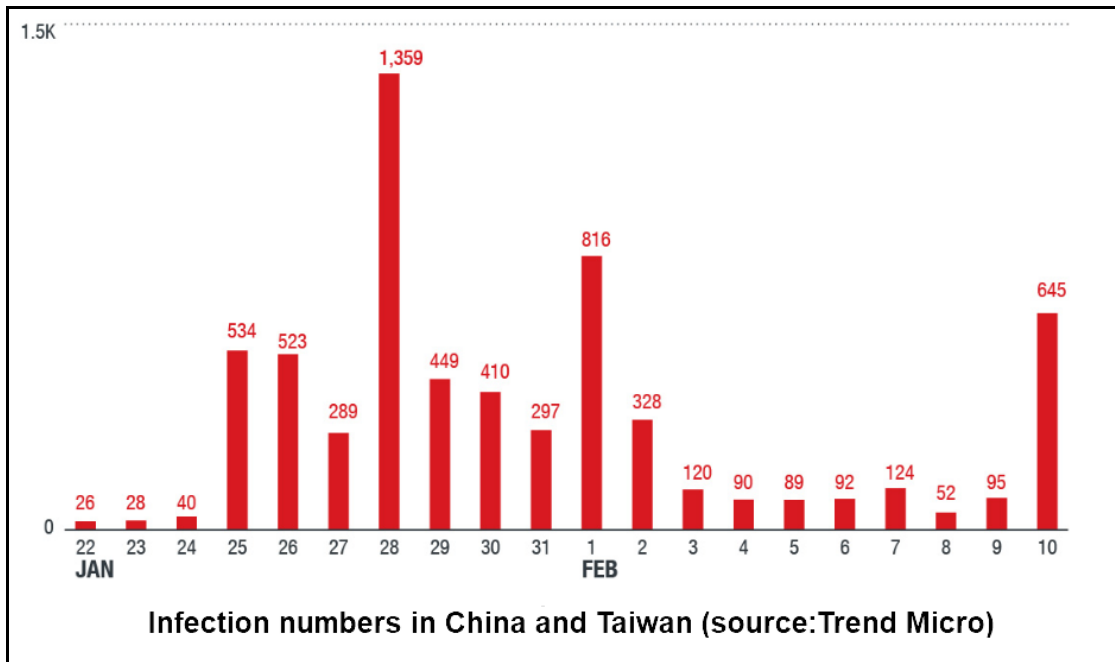


臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 5 月

一、事件簡介

1. 在 2019/2 中旬趨勢科技研究員在掃描中國、台灣、義大利與香港的漏洞主機時，發現一個新型態攻擊工具包結合了木馬與工具來散播挖礦程式與竊取資料，並且會透過 Internet 與區域網路散播自己，下圖為 2019/1/22~2019/2/10 中國與台灣每日受感染的主機數量統計。



2. 在成功地侵入受害主機後，多階段的感染過程會使用趨勢科技稱為 Trojan.Win32.INFOSTEAL.ADS 的惡意程式來開始，它將會連線 C2 伺服器來傳送主機資訊，並且下載惡意程式的負載(payload)。
3. 在學術網路內，INFOSTEAL 惡意程式的偵測規則為「MALWARE-CNC Win.Trojan.Fakewmi variant outbound connection attempt」，而且在 2019/3 首次偵測到有 18 件資安事件，至 2019/4 上升為 38 件，整個呈現上升趨勢。
4. 為了瞭解此類型攻擊行為可能造成的影響，本中心取得起始的惡意程式樣本來進行檢測。

二、事件檢測

1. 首先，使用一台安裝 Windows 7 64 位元作業系統的虛擬主機進行隔離環境測

試，將樣本 InfoSteal.exe(SHA256:

bdbfa96d17c2f06f68b3bcc84568cf445915e194f130b0dc2411805cf889b6cc)放於

主機上執行。在執行前，其經 Virustotal 檢測之惡意程度為 61/70。



2. 程式 InfoSteal.exe 在執行後，即於所在的資料夾中消失。觀察主機對外的網路連線狀況，發現 svchost.exe 會對外連線美國 IP:23.41.139.27:80，也發現 Process ID 908 與 1684 的程式 svchost.exe 執行時有開啟三個 port:65531~65533，連線狀態一直為 Listening。

2019/5/6 下午 03:27:05	Added	svchost.exe	TCP 192.168.195.137:49241	23.41.139.27:80
2019/5/6 下午 03:27:05	Added	svchost.exe	UDP 0.0.0.0:57020	*.*
2019/5/6 下午 03:27:20	Added	svchost.exe	UDP 0.0.0.0:54646	*.*
2019/5/6 下午 03:27:28	Added	svchost.exe	TCP 192.168.195.137:49242	23.41.139.27:80

Process Name	Process ID		Local Port	Local Address	Remote Port	Remote Address	State
svchost.exe	908	TCP	65531	0.0.0.0		0.0.0.0	Listening
svchost.exe	908	TCP	65532	0.0.0.0		0.0.0.0	Listening
svchost.exe	1684	TCP	65533	0.0.0.0		0.0.0.0	Listening

3. 檢查主機上防火牆的輸入規則設定，發現三個非系統本身預設的規則，分別為 ShareService、UDP 與 UDP2，這三個規則開啟了本機端的 65533、65532 與 65531port，允許主機上的任何程式執行時，讓任何人從遠端任何位址來進行連線，推測這些 port 的開啟為駭客的攻擊行為之一。

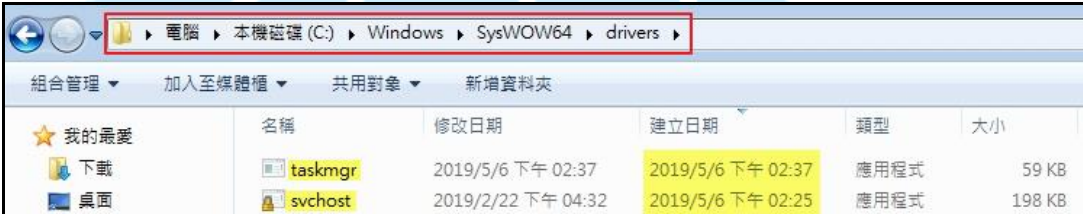
名稱	群組	已啟用	程式	本機位址	本機連接埠	遠端位址	遠端連接埠	通訊協定	執行動作
ShareService		是	任何	任何	65533	任何	任何	TCP	允許
UDP		是	任何	任何	65532	任何	任何	TCP	允許
UDP2		是	任何	任何	65531	任何	任何	TCP	允許

4. 檢視背景程式運作情形，發現有三個程式的 Description 與 Company Name 為空白，正常的程式應該有資訊，推測可能為惡意程式。

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
wmi.exe		2,152 K	7,936 K	3852		
svchost.exe	0.64	3,400 K	9,152 K	1684		
taskmgr.exe		488 K	1,496 K	388		

5. 查看程式 `svchost.exe`、`wmiex.exe` 與 `taskmgr.exe` 在主機內的檔案存放位置，發現在那些位置無法看到這些程式，要透過將資料夾選項的檢視設定修改為「不隱藏保護的作業系統檔」之後才看得到這些檔案，讓使用者不容易發現它們的存在。

修改設定後發現在 `c:\Windows\SysWOW64\drivers` 與 `c:\Windows\SysWOW64` 這兩個資料夾出現程式 `taskmgr.exe`、`svchost.exe`、`wmiex.exe` 與 `svhost.exe`，而其中 `taskmgr.exe` 與 `svchost.exe` 這兩個系統檔案所在位置不是系統預設的存放位置。另外，由建立日期判斷此為 `InfoSteal.exe` 執行後所產生的檔案，其中 `svchost.exe` 與 `svhost.exe` 兩者建立時間相同，而且檔案大小相同，推測可能為相同檔案。

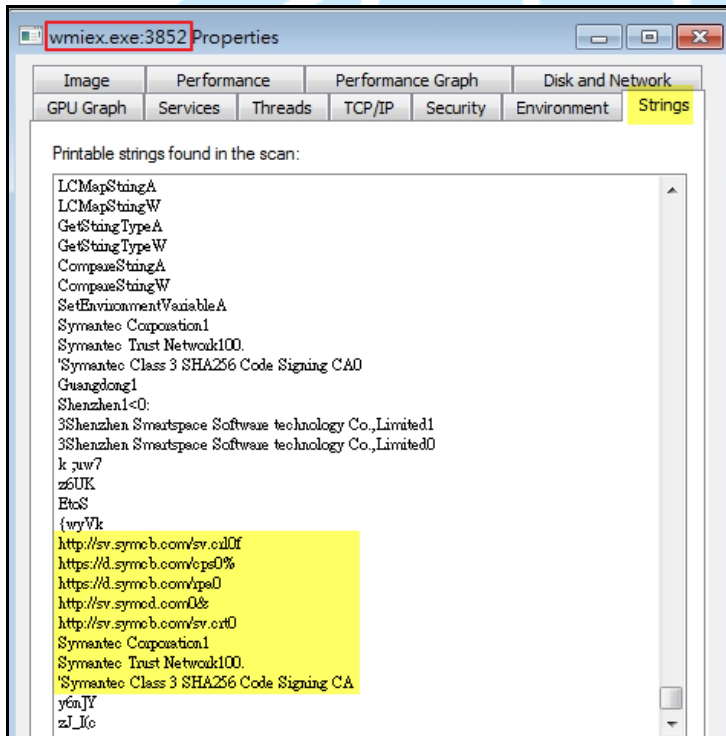
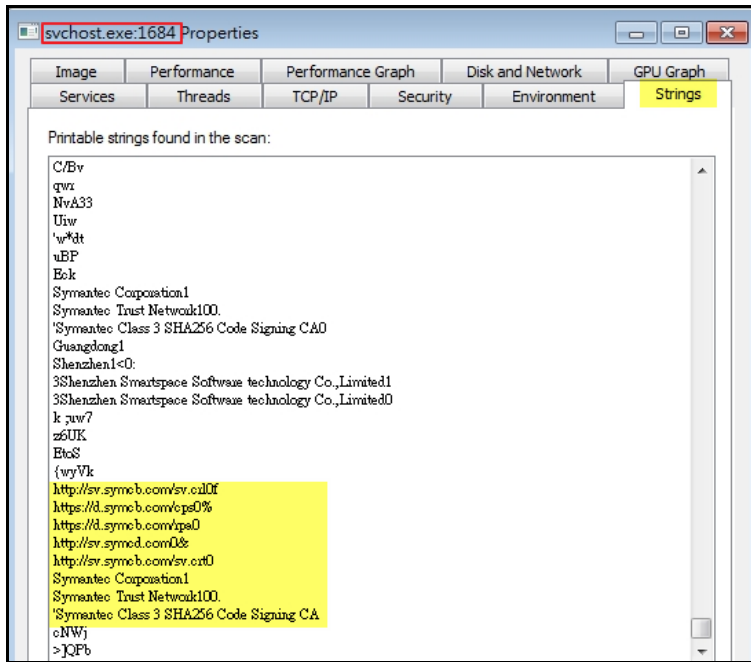


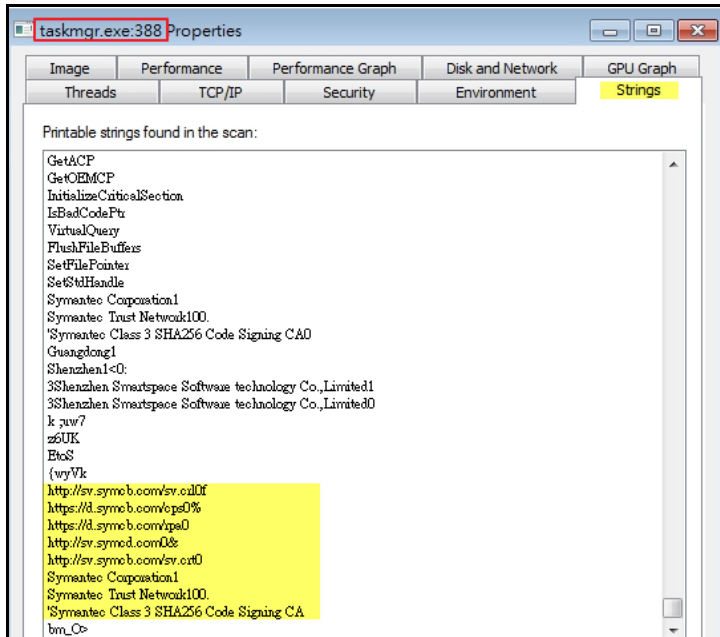
名稱	修改日期	建立日期	類型	大小
taskmgr	2019/5/6 下午 02:37	2019/5/6 下午 02:37	應用程式	59 KB
svchost	2019/2/22 下午 04:32	2019/5/6 下午 02:25	應用程式	198 KB



名稱	修改日期	建立日期	類型	大小
svhost	2019/2/22 下午 04:32	2019/5/6 下午 02:37	應用程式	198 KB
wmiex	2019/5/6 下午 02:36	2019/5/6 下午 02:36	應用程式	73 KB

6. 從程式 `svchost.exe`、`wmiex.exe` 與 `taskmgr.exe` 的屬性「Strings」內容，發現這三個程式的字串都提到賽門鐵克的憑證與憑證下載網址，推測這三個惡意程式可能被嵌入賽門鐵克的憑證，這樣竊取憑證的設計容易造成防毒軟體判定它為合法的程式。





7. 程式 taskmgr.exe、svchost.exe、wmix.exe 與 svhost.exe 經 virustotal 檢測其惡意比例分別為 50/71、63/72、56/69 與 63/72，其中 svchost.exe 與 svhost.exe 的檢測結果相同，也發現 svchost.exe 與一開始樣本 InfoSteal.exe 的 SHA256 值相同，推測惡意程式 InfoSteal.exe 執行後除了刪除自己外，另在系統檔所在資料夾中複製一份自己，並且隱藏起來，此種攻擊手法不容易讓使用者發現它的存在。

50 / 71 engines detected this file

de7dba8ef2f284e92f9ceec09599d7e4a31592b773c9642be5
bcf18f2463a3a6

taskmgr.exe

58.55 KB Size | 2019-05-06 09:17:01 UTC | 3 minutes ago

64bits assembly overlay peexe signed

63 / 72 engines detected this file

bdbfa96d17c2f06f68b3bcc84568cf445915e194f130b0dc24
11805cf889b6cc

svchost.exe

197.05 KB Size | 2019-05-06 09:04:47 UTC | 4 minutes ago

nxdomain overlay peexe signed

56 / 69 engines detected this file

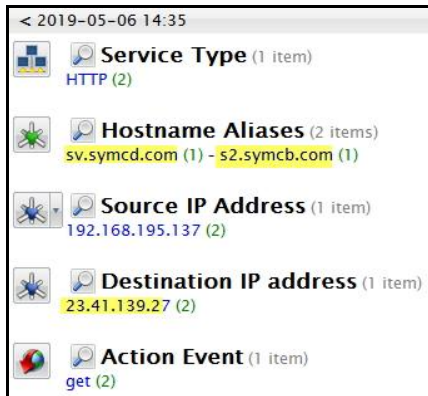
b771267551961ce840a1fbc6d65e8f5ecd0a21350387f35bbcd
4c24125ec04530

wmix.exe

72.05 KB Size | 2019-05-06 09:23:59 UTC | 3 minutes ago

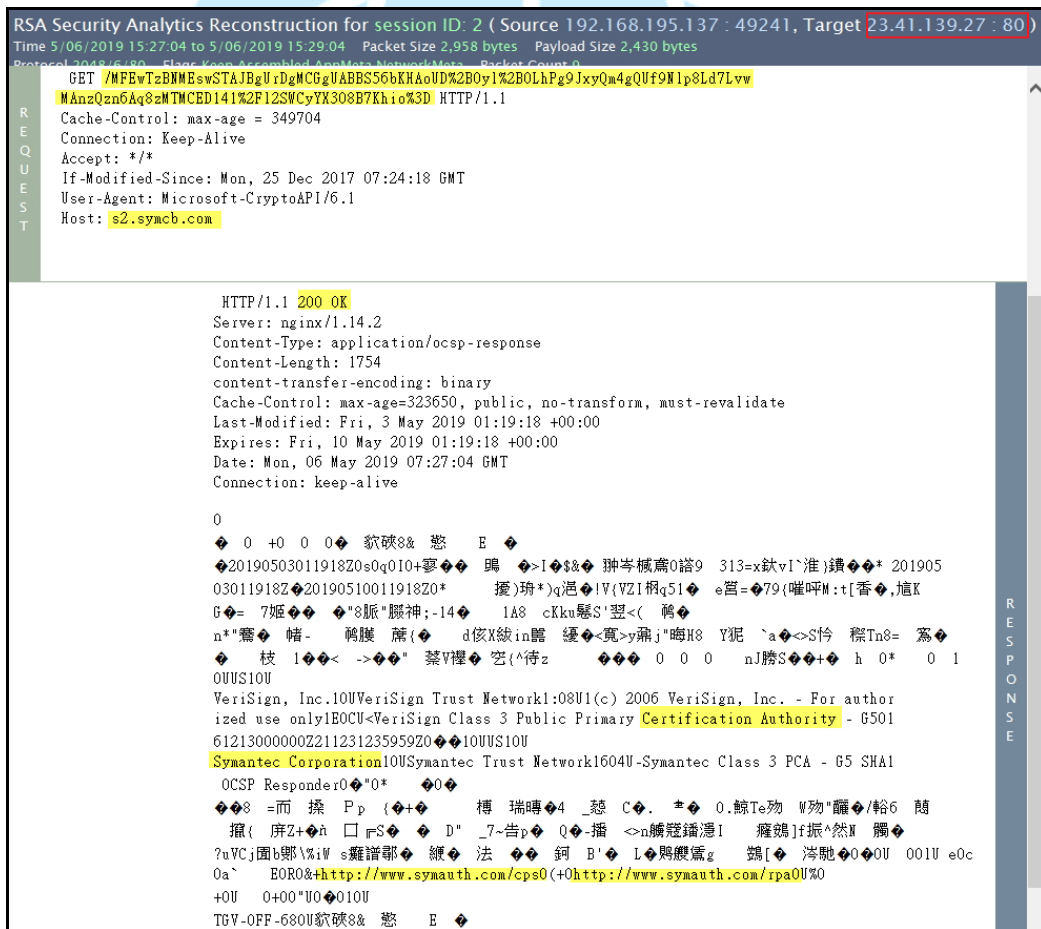
overlay peexe signed

8. 查看連線美國 IP:23.41.139.27 的封包內容，發現該 IP 會對應到兩個網址
http://s2.symcb.com 與 http://sv.symcd.com，從 IP:23.41.139.27 所回應內容，可
以得知受害主機連線至該 IP 下載賽門鐵克所核發的憑證。



< 2019-05-06 14:35

- Service Type** (1 item)
HTTP (2)
- Hostname Aliases** (2 items)
sv.symcd.com (1) - s2.symcb.com (1)
- Source IP Address** (1 item)
192.168.195.137 (2)
- Destination IP address** (1 item)
23.41.139.27 (2)
- Action Event** (1 item)
get (2)



RSA Security Analytics Reconstruction for session ID: 2 (Source 192.168.195.137 : 49241, Target 23.41.139.27 : 80)
Time 5/06/2019 15:27:04 to 5/06/2019 15:29:04 Packet Size 2,958 bytes Payload Size 2,430 bytes
Protocol 3048/6480 Flags Keep-Assembled-AppMeta-NetworkMeta- Packet Count 0

REQUEST

```

GET /MFEwTzBNMEsSwSTAJBqUrDgMCGqVABBS56bKHAoND%2B0y1%2B0LhPg9JxyQm4gQUf9N1p8Ld7Lvw
MAnzQzn6Aq8zMTMCBD141%2F12SWCyYX308B7Kha%3D HTTP/1.1
Cache-Control: max-age = 349704
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Mon, 25 Dec 2017 07:24:18 GMT
User-Agent: Microsoft-CryptoAPI/6.1
Host: s2.symcb.com
    
```

RESPONSE

```

HTTP/1.1 200 OK
Server: nginx/1.14.2
Content-Type: application/ocsp-response
Content-Length: 1754
content-transfer-encoding: binary
Cache-Control: max-age=323650, public, no-transform, must-revalidate
Last-Modified: Fri, 3 May 2019 01:19:18 +00:00
Expires: Fri, 10 May 2019 01:19:18 +00:00
Date: Mon, 06 May 2019 07:27:04 GMT
Connection: keep-alive

0
0 +0 0 0 0 欵磔& 愍 E
02019050301191820s0q010+藪 踴 >I $% 狎岑械篇0譜9 313=x欵vI`准 }鑽* 201905
03011918Z020190510011918Z0* 攬)琦*)q馮!V{VZI桐q51 e筥=79(嗶呼M:t[香,旭K
G= 7姬 8脈* 颯神;-14 1A8 cKku懸S'翌<( 鴉
n*"霽 帽- 鴉護 蔗{ d倭X綫in歸 縷<覓>y鼎j"啞H8 Y泥 `a<->S怜 糈Tn8= 蕊
枝 1<<-> 蔡V櫻 空(^待z 0 0 0 nJ勝S++ h 0* 0 1
0UVS10U
VeriSign, Inc.10UVeriSign Trust Network1:08U1(c) 2006 VeriSign, Inc. - For author
ized use only!E0CU<VeriSign Class 3 Public Primary Certification Authority - 6501
6121300000Z211231235959Z010UVS10U
Symantec Corporation10USymantec Trust Network1604U-Symantec Class 3 PCA - G5 SHA1
OCSP Responder0*0*
8 =而 捺 Pp {+ 樽 瑞暉4 _慈 C. * 0.鯨Te殉 W殉"釀/輪6 蘭
擢{ 庠Z+â □ F$ D" _7-峇p Q-播 <n鱗鏗鑄I 癩鷄]f振^然M 觸
?nVCj團b鄧\%iW s癩譜耶 縷 法 鈞 B' L 鸚鵡縷g 鸚 [ 洋馳00UV 001U e0c
0a` E0R0&+http://www.symauth.com/cps0(+0http://www.symauth.com/rpa0U%
+0V 0+00*U0010U
TGV-OFF-680U欵磔& 愍 E
    
```


cmd.exe (3988)	cmd /c start /b sc start Schedule&ping localhost&sc query Schedule findstr RUNNING&&(schtasks /del...
sc.exe (1972)	sc start Schedule
PING.EXE (1748)	ping localhost
sc.exe (3344)	sc query Schedule
findstr.exe (3360)	findstr RUNNING
schtasks.exe (2036)	schtasks /delete /TN WebServers /f
schtasks.exe (4016)	schtasks /create /ru system /sc MINUTE /mo 50 /ST 07:00:00 /TN WebServers /tr "cmd.exe /c c:\window...
schtasks.exe (2320)	schtasks /run /TN WebServers
net.exe (2140)	net start WebServers
net1.exe (2740)	C:\Windows\system32\net1 start WebServers

```
PID4016 C:\Windows\SysWOW64\schtasks.exe
schtasks /create /ru system /sc MINUTE /mo 50 /ST 07:00:00 /TN WebServers /tr
"cmd.exe /c c:\windows\SysWOW64\wmiexec.exe"
```

InfoSteal.exe 執行後也會呼叫 cmd.exe(PID 624)來強制結束排程 svchost.exe、svhhost.exe 與 svvhost.exe 等程序，並且移動 svvhost.exe 與 svchost.exe 至 c:\windows\temp 內，而且會刪除位於 c:\windows\system32 內的 svhhost.exe 與位於 c:\windows\syswow64 內的 svhhost.exe。

cmd.exe (624)	cmd /c taskkill /f /im svchost.exe /im svhhost.exe /im svvhost.exe & move /y c:\windows\temp\svhst...
taskkill.exe (4092)	taskkill /f /im svchost.exe /im svhhost.exe /im svvhost.exe

```
PID624 C:\Windows\SysWOW64\cmd.exe
cmd /c taskkill /f /im svchost.exe /im svhhost.exe /im svvhost.exe & move /y c:
\windows\temp\svvhost.exe c:\windows\temp\svchost.exe & del c:\windows
\system32\svhhost.exe & del c:\windows\syswow64\svhhost.exe
```

接著 cmd.exe 會執行一個判斷程序，當 process 名稱為 svchost.exe、svhhost.exe 或 svvhost.exe 時終止該程序的執行。之後 cmd.exe 會透過 WMIC.exe 去執行下列判斷程序：(1)如果 Process 的執行路徑在%drivers%的路徑內，而且檔案名稱為 taskmgr.exe，則結束該程序(2) 如果 Process 的執行路徑在%drivers%的路徑內，而且檔案名稱為 svchost.exe，則結束該程序(3) 如果 Process 的執行路徑在%emp%的路徑內，而且檔案名稱為 svchost.exe，則結束該程序，推測此行為是駭客用來偵測主機是否曾經感染過此惡意程式的判斷程序。

cmd.exe (3664)	cmd /c wmic process where "name='svchost.exe' or name='svhhost.exe' or name='svvhost.exe'" delete
WMIC.exe (2408)	wmic process where "name='svchost.exe' or name='svhhost.exe' or name='svvhost.exe'" delete
cmd.exe (3780)	cmd /c wmic process where "ExecutablePath like '%drivers%' and name='taskmgr.exe'" delete & wmic ...
WMIC.exe (492)	wmic process where "ExecutablePath like '%drivers%' and name='taskmgr.exe'" delete
WMIC.exe (2820)	wmic process where "ExecutablePath like '%drivers%' and name='svchost.exe'" delete
WMIC.exe (3704)	wmic process where "ExecutablePath like '%emp%' and name='svchost.exe'" delete

InfoSteal.exe 執行時也會透過 cmd.exe 來執行 netsh 指令，開啟 3 個 65531~65533 的 port，這些 port 的規則名稱分別為 UDP2、UDP 與 ShareService。

cmd.exe (1908)	cmd /c netsh interface ipv6 install&netsh firewall add portopening tcp 65532 UDP&netsh interface port...
netsh.exe (1344)	netsh interface ipv6 install
netsh.exe (3284)	netsh firewall add portopening tcp 65532 UDP
netsh.exe (3992)	netsh interface portproxy add v4tov4 listenport=65532 connectaddress=1.1.1.1 connectport=53
netsh.exe (3784)	netsh firewall add portopening tcp 65531 UDP2
netsh.exe (3060)	netsh interface portproxy add v4tov4 listenport=65531 connectaddress=1.1.1.1 connectport=53
netsh.exe (2828)	netsh firewall add portopening tcp 65533 ShareService

接著會透過 cmd.exe 執行 schtasks.exe 來強制刪除任務名稱為 Ddrivers 的排程，之後建立一個新的 Ddrivers 排程工作，來執行

c:\windows\SysWOW64\drivers 資料夾內的 svchost.exe。

cmd.exe (2144)	cmd /c start /b sc start Schedule&ping localhost&sc query Schedule findstr RUNNING&&(schtasks /del...
sc.exe (3624)	sc start Schedule
PING.EXE (1860)	ping localhost
sc.exe (1852)	sc query Schedule
findstr.exe (3308)	findstr RUNNING
schtasks.exe (3928)	schtasks /delete /TN Ddrivers /f
schtasks.exe (3812)	schtasks /create /ru system /sc MINUTE /mo 50 /ST 07:00:00 /TN Ddrivers /tr "cmd.exe /c c:\windows\Sy...
schtasks.exe (3644)	schtasks /run /TN Ddrivers
net.exe (3816)	net start Ddriver
net1.exe (2300)	C:\Windows\system32\net1 start Ddriver

```
PID3812 C:\Windows\SysWOW64\schtasks.exe
schtasks /create /ru system /sc MINUTE /mo 50 /ST 07:00:00 /TN Ddrivers /tr
"cmd.exe /c c:\windows\SysWOW64\drivers\svchost.exe"
```

(2) svchost.exe(PID:908)執行後

它會呼叫 taskeng.exe 來執行 cmd.exe，而 cmd.exe 會分別執行位於 c:\windows\SysWOW64\wmiex.exe 與 c:\windows\SysWOW64\drivers\svchost.exe 的兩個程式，來開始 WebServers 與 Ddriver 兩個工作排程。

svchost.exe (908)	C:\Windows\system32\svchost.exe -k netsvcs
taskeng.exe (1280)	taskeng.exe (359BB66A-FCB7-4A6C-ABCE-7E0DF6B3B573)
cmd.exe (3604)	cmd.exe /c c:\windows\SysWOW64\wmiex.exe
wmiex.exe (1064)	c:\windows\SysWOW64\wmiex.exe
net.exe (1468)	net start WebServers
net1.exe (3456)	C:\Windows\system32\net1 start WebServers
cmd.exe (2448)	cmd.exe /c c:\windows\SysWOW64\drivers\svchost.exe
svchost.exe (896)	c:\windows\SysWOW64\drivers\svchost.exe
net.exe (3884)	net start Ddriver
net1.exe (3356)	C:\Windows\system32\net1 start Ddriver

(3) wmiex.exe(PID:3852)執行後

它會呼叫 wmic.exe(PID:3180)來取得 UUID 與 macaddress 資訊。

wmiex.exe (3852)	c:\windows\SysWOW64\wmiex.exe
wmic.exe (3180)	wmic csproduct get UUID
wmic.exe (3948)	wmic nic where netconnectionid!=NULL get macaddress

(4) svchost.exe(PID:1684)執行後

在 c:\windows\SysWOW64\drivers 資料夾內的 svchost.exe 執行後，它會呼

叫位於同一個資料夾內的程式 taskmgr.exe，接著會使用 cmd.exe 執行 8 次 WMIC.exe，來檢查 taskmgr.exe、svchost.exe、explorer.exe、spoolsv.exe、conhost.exe、csrss.exe、services.exe 與 msdtc.exe 等 8 個程式的執行路徑，若不符合則終止該程式的程序。

之後會使用 cmd.exe 一直重複執行這 8 次的 WMIC.exe。此外，它也會透過執行 wmic.exe 來取得 UUID、macaddress 與 VideoController 等資訊。

Process	Command
svchost.exe (1684)	c:\windows\SysWOW64\drivers\svchost.exe
taskmgr.exe (388)	"c:\windows\SysWOW64\drivers\taskmgr.exe"
cmd.exe (1992)	cmd /c wmic process where "name='taskmgr.exe' and executablepath<>'%System
WMIC.exe (3732)	wmic process where "name='taskmgr.exe' and executablepath<>'C:\\window
WMIC.exe (3216)	wmic process where "name='svchost.exe' and executablepath<>'C:\\windows
WMIC.exe (1712)	wmic process where "name='explorer.exe' and executablepath<>'C:\\window
WMIC.exe (2152)	wmic process where "name='spoolsv.exe' and executablepath<>'C:\\window
WMIC.exe (828)	wmic process where "name='conhost.exe' and executablepath<>'C:\\window
WMIC.exe (3292)	wmic process where "name='csrss.exe' and executablepath<>'C:\\windows\\
WMIC.exe (2524)	wmic process where "name='services.exe' and executablepath<>'C:\\window
WMIC.exe (2632)	wmic process where "name='msdtc.exe' and executablepath<>'C:\\windows\\
wmic.exe (372)	wmic csproduct get UUID
wmic.exe (3380)	wmic nic where netconnectionid!=NULL get macaddress
Wmic.exe (1516)	Wmic Path Win32_VideoController Get Description
powershell.exe (3904)	powershell -ep bypass -nop -c "(Get-EventLog -LogName 'Security' -After (get-d

10. 檢視主機啟動後程式執行設定、排程工作與服務內容，發現

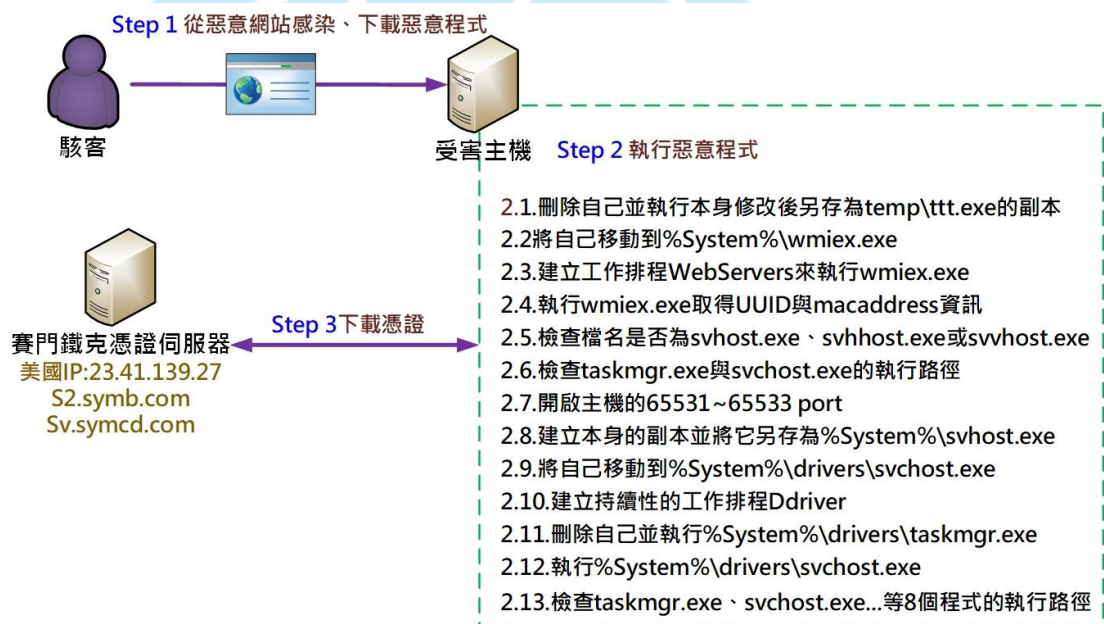
c:\windows\syswow64\drivers 資料夾內的 svchost.exe 與 c:\windows\syswow64 資料夾內的 wmiex.exe 在主機重新啟動後會自動執行，而且也列入工作排程與服務內容之一。

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
Ddriver			c:\windows\syswow64\drivers\svchost.exe	2016/6/30 下午 02:21
vm				2016/8/26 上午 05:21
WebServers			c:\windows\syswow64\wmiex.exe	2016/6/30 下午 02:21

Autorun Entry	Description	Publisher	Image Path	Timestamp
Task Scheduler				
\Ddrivers			c:\windows\syswow64\drivers\svchost.exe	2016/6/30 下午 02:21
\GoogleUpdateTask...	Google 安裝程式	Google Inc.	c:\program files (x86)\google\update\googleupdate...	2017/4/22 上午 09:31
\GoogleUpdateTask...	Google 安裝程式	Google Inc.	c:\program files (x86)\google\update\googleupdate...	2017/4/22 上午 09:31
\Microsoft\Windows...	Microsoft Malware Prote...	Microsoft Cor...	c:\program files\windows defender\mpcmdrun.exe	2009/7/14 上午 07:53
\Microsoft\Windows...			c:\windows\syswow64\dfdwiz.exe	
\Microsoft\Windows...			c:\windows\system32\gathernetworkinfo.vbs	2009/6/11 上午 04:36
\Microsoft\Windows...	Windows Media Player ...	Microsoft Cor...	c:\program files\windows media player\wmpnscfg.exe	2009/7/14 上午 08:24
\WebServers			c:\windows\syswow64\wmiex.exe	2016/6/30 下午 02:21

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\System\CurrentControlSet\Services				
AppIDSvc	判斷並確定...		c:\windows\syswow64\appidsvc.dll	2019/5/6 下午 02:37
bthserv	Bluetooth 服...		c:\windows\syswow64\bthserv.dll	
CscService	離線檔案服...		c:\windows\syswow64\cscsvc.dll	
Ddriver	Provides abil...		c:\windows\syswow64\drivers\svchost.exe	2016/6/30 下午 02:21
GoogleChromeElev...	Google Chro...	Google Inc.	c:\program files (x86)\google\chrome\application\74.0.3729.131\elevation_service.exe	2019/4/29 下午 01:00
gupdate	這會持續更...	Google Inc.	c:\program files (x86)\google\update\googleupdate.exe	2017/4/22 上午 09:31
gupdatem	這會持續更...	Google Inc.	c:\program files (x86)\google\update\googleupdate.exe	2017/4/22 上午 09:31
MpsSvc	Windows 防...		c:\windows\syswow64\mpssvc.dll	
nsi	此服務可將...		c:\windows\syswow64\nsisvc.dll	
p2pimsvc	提供對等名...		c:\windows\syswow64\pnrpmsvc.dll	
PeerDistSvc	此服務會從...		c:\windows\syswow64\peerdistsvc.dll	
RpcSs	RPCSS 服...		c:\windows\syswow64\rpcss.dll	
WebServers	forwards it to...		c:\windows\syswow64\wmiex.exe	2016/6/30 下午 02:21
WinDefend	提供對間諜...	Microsoft ...	c:\program files\windows defender\mpsvc.dll	2009/7/14 上午 09:29
WMPNetworkSvc	與其他網路...	Microsoft ...	c:\program files\windows media player\wmpnetwk.exe	2010/11/20 下午 07:18

三、事件攻擊行為示意圖



1. 使用者從惡意網站感染、下載惡意程式。
2. 惡意程式在受害主機上被執行後，產生下列各個行為：
 - (1) 刪除自己並執行本身修改後另存為 temp\ttt.exe 的副本。
 - (2) 將自己移動到%system%\wmiex.exe。
 - (3) 建立工作排程 WebServers 來執行 wmiex.exe。
 - (4) 執行 wmiex.exe 取得 UUID 與 macaddress 資訊。
 - (5) 檢查檔名為 svchost.exe、svhhost.exe 或 svvhost.exe 時，則終止程序。

- (6)檢查 taskmgr.exe 與 svchost.exe 的執行路徑，若符合則終止程序。
 - (7)開啟主機的 65531~65533 port。
 - (8)建立本身的副本並將它另存為%system%\svchost.exe。
 - (9)將自己移動到%system%\drivers\svchost.exe。
 - (10)建立持續性的工作排程 Ddriver。
 - (11)刪除自己並執行%system%\drivers\taskmgr.exe。
 - (12)執行%system%\drivers\svchost.exe。
 - (13)檢查 taskmgr.exe、svchost.exe、explorer.exe...等 8 個程式的執行路徑，
若不符合則終止程序。
- 3.連線賽門鐵克憑證伺服器(美國 IP:23.41.139.27)下載憑證。

四、建議與總結

1. 本個案的攻擊手法主要在感染主機後，將惡意程式安裝於 Windows 系統檔存放的資料夾內，會檢查是否有相關的舊版本軟體存在，透過刪除與初始化將這些舊版本軟體、檔案和程序重新安裝與設定，來讓受害主機感染最新版的惡意軟體。
2. 該惡意程式在執行後，會利用自己本身的資源建立一個 c:\windows\temp\ttt.exe 來啟動更新作業。
3. 它會檢查檔案名稱是否為 svchost.exe、svhhost.exe 或 svvhost.exe，如果不是，則會終止所有舊版的惡意軟體、啟用防火牆，並且開放 port。
4. 它會在驅動程式中植入修改後的自身副本，並建立一個工作排程來執行 wmiex.exe，作為線上連線來傳送系統資訊。
5. 由於它開啟 65531~65533port，能讓任何程式從任何來源來使用這些 port，容易讓駭客為遠端管理植入駭客工具於主機內。
6. 放於主機系統檔資料夾內的惡意程式，一般是隱藏狀態，如果不解除隱藏

保護，則使用者看不到它們的存在，將使它們持續潛伏在受害主機內來竊取資訊。

7. 關於本個案之資安防護措施，有下列幾點建議提供參考。

- (1) 不隨意瀏覽不明來源的網站。
- (2) 不隨意點選不明來源的連結。
- (3) 定期更新系統、修補漏洞與更新病毒碼。
- (4) 定期檢視主機 port 開啟的狀況。
- (5) 定期使用防毒軟體進行全系統的完整掃描。

五、相關報導

1. Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect, Propagate via Vulnerability

<https://blog.trendmicro.com/trendlabs-security-intelligence/monero-miner-malware-uses-radmin-mimikatz-to-infect-propagate-via-vulnerability/>



← → ↻ 🔒 Trend Micro Inc. [US] | <https://blog.trendmicro.com/trendlabs-...> 🔍 ⌘ ⚙️ ⌂ 🌐 📧

Go to...

Home » Exploits » Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect, Propagate via Vulnerability

Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect, Propagate via Vulnerability

Posted on: February 20, 2019 at 5:04 am | Posted in: Exploits, Malware, Targeted Attacks, Vulnerabilities
Author: Trend Micro

 44   

By Don Ovid Ladores, Michael Jhon Ofiaza and Gilbert Sison

Between the last week of January to February, we noticed an increase in hack tool installation attempts that dropped seemingly random files into the Windows directory. Initially appearing unrelated, analysis showed the final payload to be a **Monero** cryptocurrency-mining malware variant as it scans for open port 445 and exploit a Windows **SMB Server Vulnerability MS17-010** (patched in 2017) for its infection and propagation routines, targeting companies in China, Taiwan, Italy, and Hong Kong.

MIMIKATZ has been used with other hack tools and **coinmining-malware in previous routines** to collect user accounts and system credentials, while malicious actors have used RADMIN tools **to gain admin rights and other malware into targeted systems**. However, this combination of RADMIN and MIMIKATZ becomes a concern for data exfiltration of enterprise assets and information because of the randomly named and seemingly-valid Windows functions that may go undetected. Also,

