個案分析-

SQL 資料庫主機感染 Cry36 勒索病毒事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106 年 7 月

I. 事件簡介

1. 本事件為教育部一台執行計畫用的 SQL 資料庫主機發生中毒現象。
2. 該主機為一台虛擬主機，所安裝的系統為 Windows Server 2008 R2 系統。
3. 該主機在 106 年 4 月底才完成系統建置作業，主要提供廠商以固定 IP 透過 3389 port 方式從遠端連線主機。
4. 本單位取得該虛擬主機的樣本後，以還原系統的方式進行研究分析。

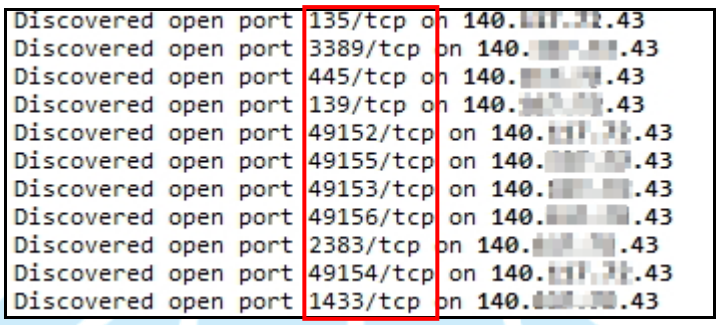
II. 事件檢測

1. 以使用者身分登入後，桌面出現「ALL YOUR FILES ARE ENCRYPTED」所有檔案已被加密的桌布圖片，所有被加密的檔案之副檔名皆為.s79ob，若以管理者身分登入系統，無法看到這些資訊。

2. 從被加密的檔案名稱觀察，其檔案名稱範例如下:

   原檔案名稱.id-1883958650_[mk.predator@aol.com].s79ob，發現其檔案命名方式與 Cry36 勒索病毒相似，皆包含受害者的識別 id、犯罪者的電子郵件地址和 5 個隨機字母與數字混合延伸的副檔名。

3. 以 Nmap 工具檢視受測主機對外的連接埠資訊，發現 135、139、445、1433、2383、3389 與 49152~49156 等 11 個連接埠為開啟狀態。

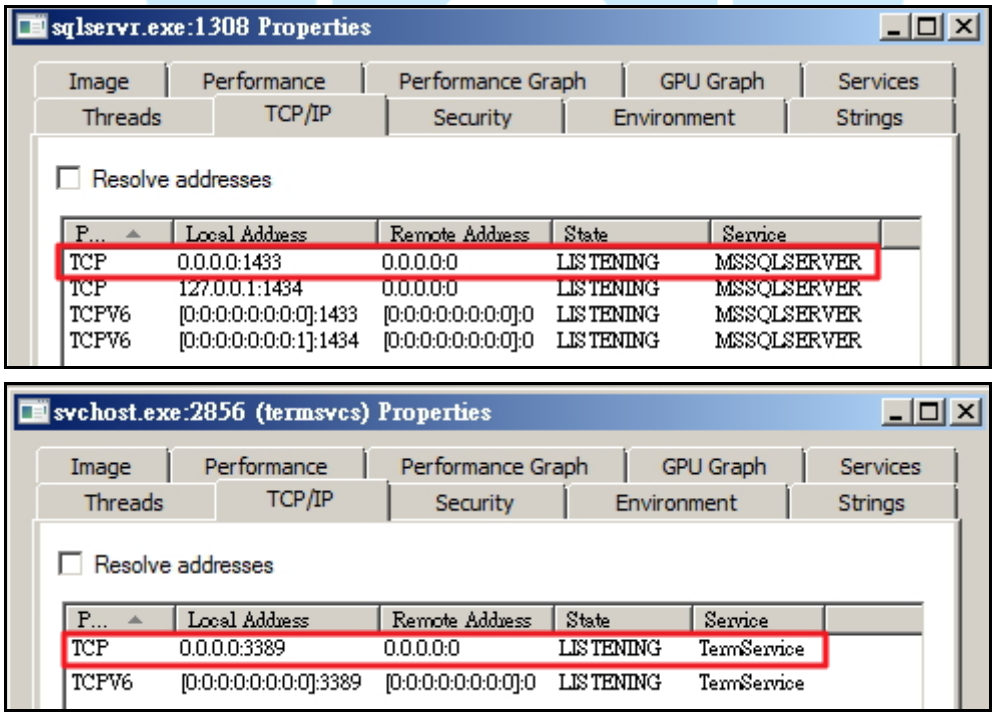


4. 以 Currports 工具檢測，發現有三個 IP 位址 122.114.51.141、221.236.172.235 與 223.100.138.14 對受測主機進行 1433 port 大量連線，查詢這三個 IP 來源位址發現皆來自於中國大陸，又發現有另一個來自荷蘭的 IP:5.39.218.17 與中國 IP:223.100.138.14 試圖透過 3389port 對受測主機進行連線，可見這兩個 port 容易變成外部電腦攻擊的管道，建議管理者檢視這兩個 port 開啟之用途。

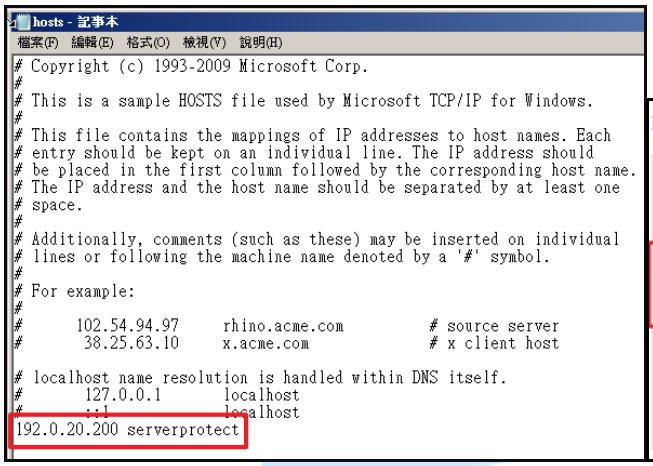
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Process]	0	TCP	140. .43	1433	122.114.51.141	50023	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	51049	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	51521	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	51640	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	51924	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52006	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52103	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52147	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52183	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52236	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52356	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52436	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	52566	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	53600	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	53748	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	53977	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	221.236.172.235	54026	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	54543	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	58668	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	59457	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	59616	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	63886	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	63927	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	64301	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	64889	TIME_WAIT
[System Process]	0	TCP	140. .43	1433	122.114.51.141	62586	TIME_WAIT

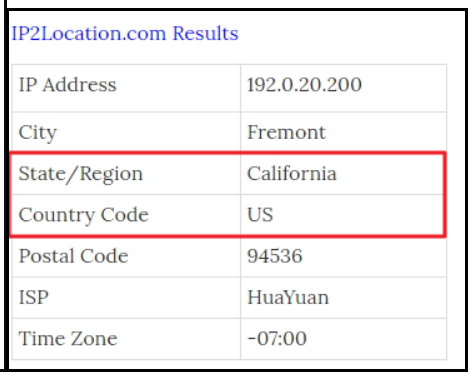
Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0		140. .43	1433	223.100.138.14	63355	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63318	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63082	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63132	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63437	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63344	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63414	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63401	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63424	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63370	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63384	TIME_WAIT
[System Proc...	0	TCP	140. .43	1433	223.100.138.14	63450	TIME_WAIT
lsass.exe	552	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING
lsass.exe	552	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING
msmdsrv.exe	1340	TCP	0.0.0.0	2383	0.0.0.0	0	LISTENING
msmdsrv.exe	1340	TCPV6	[0:0:0:0:0:0:0:0]	2383	[0:0:0:0:0:0:0:0]	0	LISTENING
services.exe	544	TCP	0.0.0.0	49156	0.0.0.0	0	LISTENING
services.exe	544	TCPV6	[0:0:0:0:0:0:0:0]	49156	[0:0:0:0:0:0:0:0]	0	LISTENING
snmp.exe	1808	UDP	0.0.0.0	161	*	*	
snmp.exe	1808	UDPV6	[0:0:0:0:0:0:0:0]	161	*	*	
sqlservr.exe	1308	TCP	0.0.0.0	1433	0.0.0.0	0	LISTENING
sqlservr.exe	1308	TCP	127.0.0.1	1434	0.0.0.0	0	LISTENING
sqlservr.exe	1308	TCPV6	[0:0:0:0:0:0:0:0]	1433	[0:0:0:0:0:0:0:0]	0	LISTENING
sqlservr.exe	1308	TCPV6	[0:0:0:0:0:0:0:1]	1434	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	740	TCP	0.0.0.0	135	0.0.0.0	0	LISTENING
svchost.exe	2856	TCP	0.0.0.0	3389	0.0.0.0	0	LISTENING
svchost.exe	824	TCP	0.0.0.0	49153	0.0.0.0	0	LISTENING
svchost.exe	872	TCP	0.0.0.0	49154	0.0.0.0	0	LISTENING
svchost.exe	872	UDP	0.0.0.0	500	*	*	
svchost.exe	872	UDP	0.0.0.0	4500	*	*	
svchost.exe	740	TCPV6	[0:0:0:0:0:0:0:0]	135	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	2856	TCPV6	[0:0:0:0:0:0:0:0]	3389	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	824	TCPV6	[0:0:0:0:0:0:0:0]	49153	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	872	TCPV6	[0:0:0:0:0:0:0:0]	49154	[0:0:0:0:0:0:0:0]	0	LISTENING
svchost.exe	872	UDPV6	[0:0:0:0:0:0:0:0]	500	*	*	
svchost.exe	872	UDPV6	[0:0:0:0:0:0:0:0]	4500	*	*	
svchost.exe	1012	UDP	0.0.0.0	5355	*	*	
svchost.exe	2856	TCP	140. .43	3389	5.39.218.17	31594	ESTABLISHED
System	4	TCP	0.0.0.0	445	0.0.0.0	0	LISTENING

5. 從 Process Explorer 檢視背景程式，發現程式 sqlservr.exe 開啟 1433 port，該 Port 一般為 SQL 資料庫遠端管理連線用，而 svchost.exe 開啟 3389 port。



6. 從 Hosts 檔案中發現到一個 IP:192.0.20.200，對應到 serverprotect 的網域，經檢查該 IP 屬於美國加州。





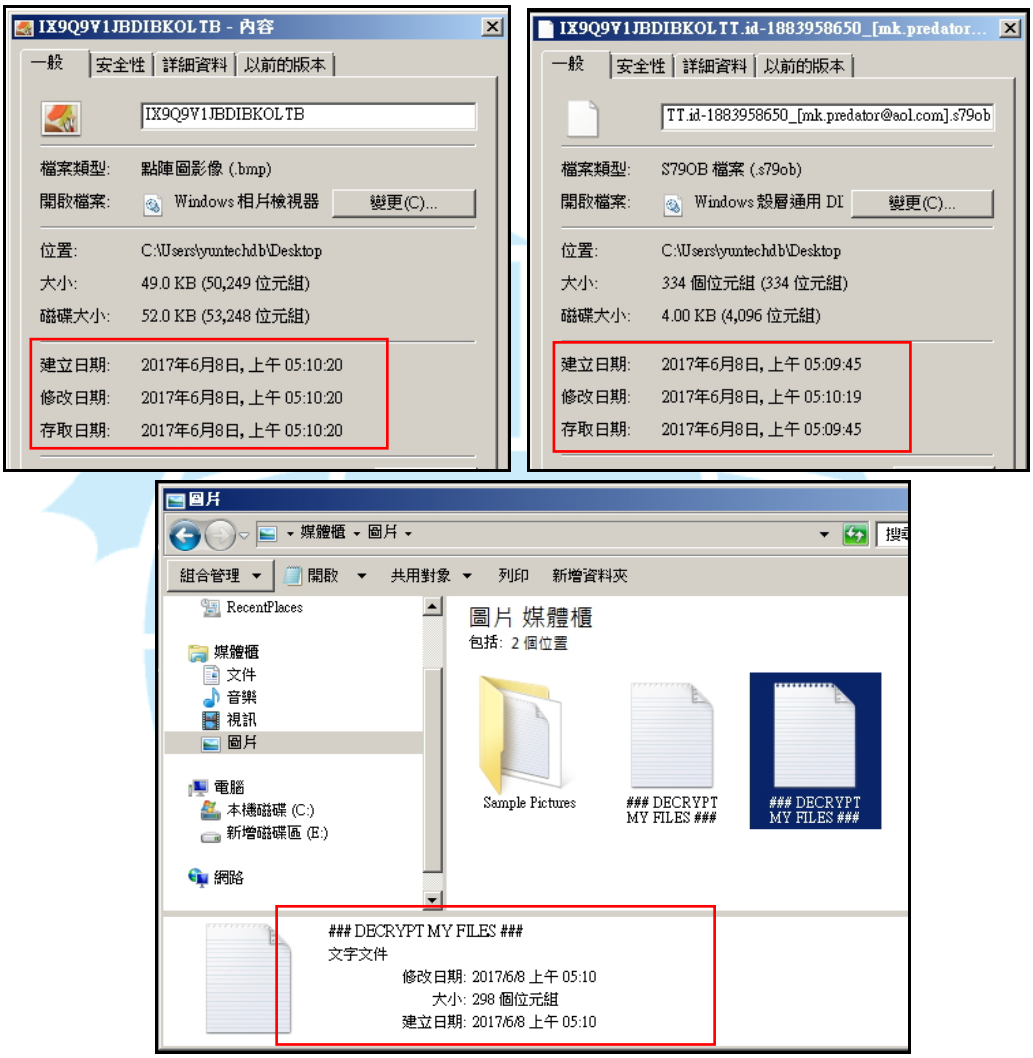
7. 從事件檢視紀錄發現，從 106 年 6 月 2 日開始該主機陸續出現下列可疑 IP 的連線:

185.158.112.184(俄羅斯莫斯科)、216.218.206.66(美國加州)連線 3 次、184.105.247.194(美國加州)、202.137.10.190(印尼雅加達)、184.105.139.67(美國加州)、185.129.148.234(拉脫維亞裡加)、184.105.247.196(美國加州)、74.82.47.5(美國加州)、185.56.82.42(荷蘭阿姆斯特丹)2 次、66.240.219.146(美國加州)、31.207.47.95(荷蘭阿姆斯特丹)，

其中在 106 年 6 月 4-8 日期間有許多帳戶無法登入訊息，所使用的帳戶名稱多達數十種，如 LOVE、DOCUMENTS、CAD、JIAZHEN、…，可見駭客攻擊行為。

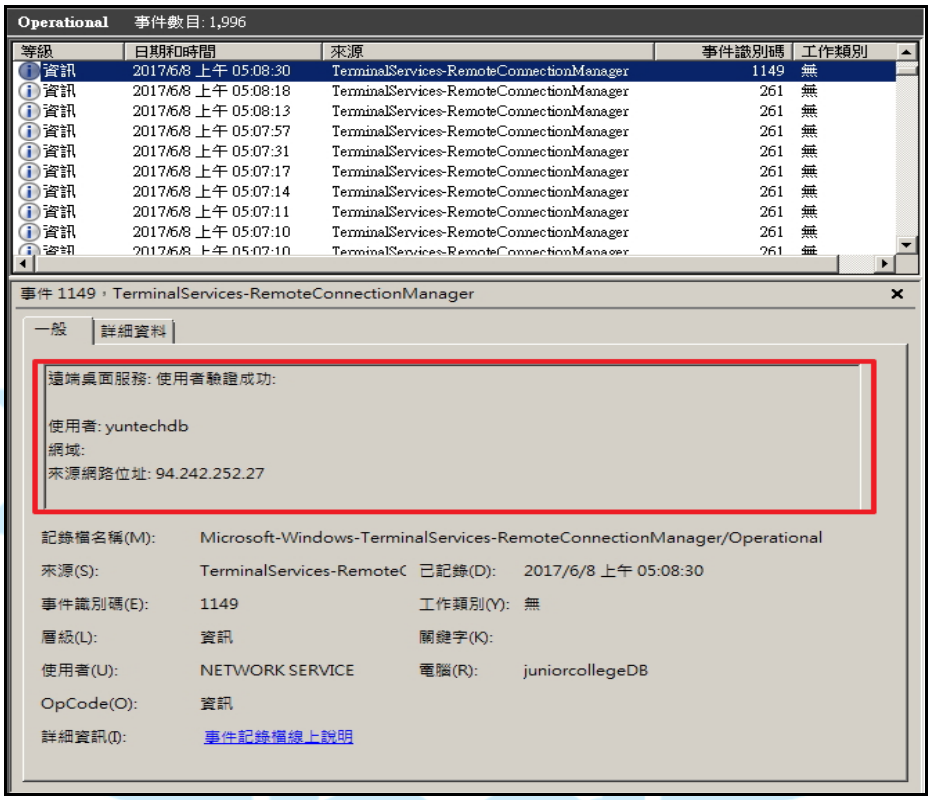
Time	Source	Categ...	Event ID	Computer	Record Length	Event Description
2017/6/8 上午 05:05:31	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	372	帳戶無法登入。
2017/6/8 上午 05:05:38	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	352	帳戶無法登入。
2017/6/8 上午 05:05:50	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:05:54	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:06:06	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:06:07	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:06:34	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:06:39	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	352	帳戶無法登入。
2017/6/8 上午 05:06:48	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:06:58	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	356	帳戶無法登入。
2017/6/8 上午 05:07:12	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:07:12	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:07:12	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	356	帳戶無法登入。
2017/6/8 上午 05:07:15	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:07:17	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	372	帳戶無法登入。
2017/6/8 上午 05:07:32	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:07:58	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。
2017/6/8 上午 05:08:14	Microsoft-Windows-Security-Auditing	12544	4625	juniorcollegeDB	368	帳戶無法登入。

8. 從被加密的檔案方面觀察，發現主機內所有資料夾(含桌面)都出現一個名為###DECRYPT MY FILES###.txt 的文字檔，此與 Cry36 勒索病毒的特徵相同，而且所有被加密的檔案建立日期與修改日期皆介於 106 年 6 月 8 日上午 5:09 至上午 5:10 之間，推測為駭客攻擊時間。



9. 透過 LastActivityView 工具，發現在 106 年 6 月 8 日上午 5:08 至 5:10 期間有短暫兩分鐘的使用者登入、登出紀錄，與主機內檔案被加密的時間相同，查看事件檢視器之「遠端桌面連線管理」紀錄，發現在 106 年 6 月 8 日上午 5:08 有來自盧森堡 IP:94.242.252.27 之遠端連線，以使用者名稱「yuntechdb」成功登入，推測為駭客登入時間。

Action Time	Description	Filename	Full Path	More Information
2017/6/8 下午 03:13:04	User Logoff			JUNIORCOLLEGEDB\Administrator
2017/6/8 上午 09:39:30	User Logon			WORKGROUP\Administrator
2017/6/8 上午 09:34:32	User Logoff			JUNIORCOLLEGEDB\yuntechdb
2017/6/8 上午 09:34:03	Open file or folder	Downloads	C:\Users\yuntechdb\Downloads	
2017/6/8 上午 09:33:49	View Folder in Explorer	Videos	C:\Users\Administrator\Videos	
2017/6/8 上午 09:33:48	View Folder in Explorer	Pictures	C:\Users\Administrator\Pictures	
2017/6/8 上午 09:33:45	View Folder in Explorer	Music	C:\Users\Administrator\Music	
2017/6/8 上午 09:33:42	View Folder in Explorer	Downloads	C:\Users\Administrator\Downloads	
2017/6/8 上午 09:30:50	View Folder in Explorer	Admin	C:\PerfLogs\Admin	
2017/6/8 上午 09:30:41	View Folder in Explorer	Temp	C:\Temp	
2017/6/8 上午 09:29:17	Open file or folder	IX9Q9V1JBDIBKOLTB.bmp	C:\Users\yuntechdb\Desktop\IX9Q9V1JBDIBKOLTB.bmp	
2017/6/8 上午 09:28:47	User Logon			WORKGROUP\yuntechdb
2017/6/8 上午 09:18:15	System Started			
2017/6/8 上午 05:10:44	System Shutdown			
2017/6/8 上午 05:10:29	User Logoff			JUNIORCOLLEGEDB\yuntechdb
2017/6/8 上午 05:08:32	User Logon			WORKGROUP\yuntechdb



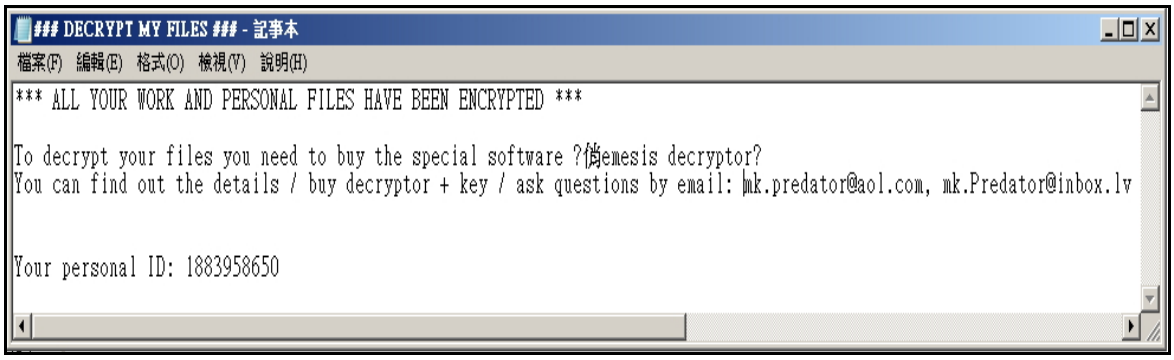
10. 使用 Redline 工具檢視測試主機 Event logs 紀錄，發現從主機系統建置完成後，陸續有下列可疑 IP 透過遠端桌面服務(RDP)方式登入系統，可疑 IP 詳列如下: 185.70.186.152(荷蘭)、82.192.65.156(荷蘭)、5.39.222.19(荷蘭)、5.39.218.17(荷蘭)、46.17.101.85(荷蘭)、93.190.138.29(荷蘭)、146.185.239.100(俄羅斯)、185.129.148.234(拉脫維亞)、46.105.107.107(法國)、188.42.253.90(中國)、178.137.89.8(烏克蘭)、94.242.252.27(盧森堡)。另外，也發現有 3 個可疑 IP 有「遠端桌面服務: 使用者驗證成功」紀錄，分別是以管理者身分登入的美國 IP:162.209.168.91 與中國 IP:58.218.213.25，以及以使用者身分登入的盧森堡 IP:94.242.252.27(駭客所用 IP)，由上列 IP 中發現荷蘭 IP:5.39.218.17 在

檢測該主機期間有再次連線狀況，又檢視受測主機發現其防火牆功能未啟動，由以上紀錄可以得知該受測主機的 RDP 連線設定與密碼強度需再加強，以免駭客再次入侵。

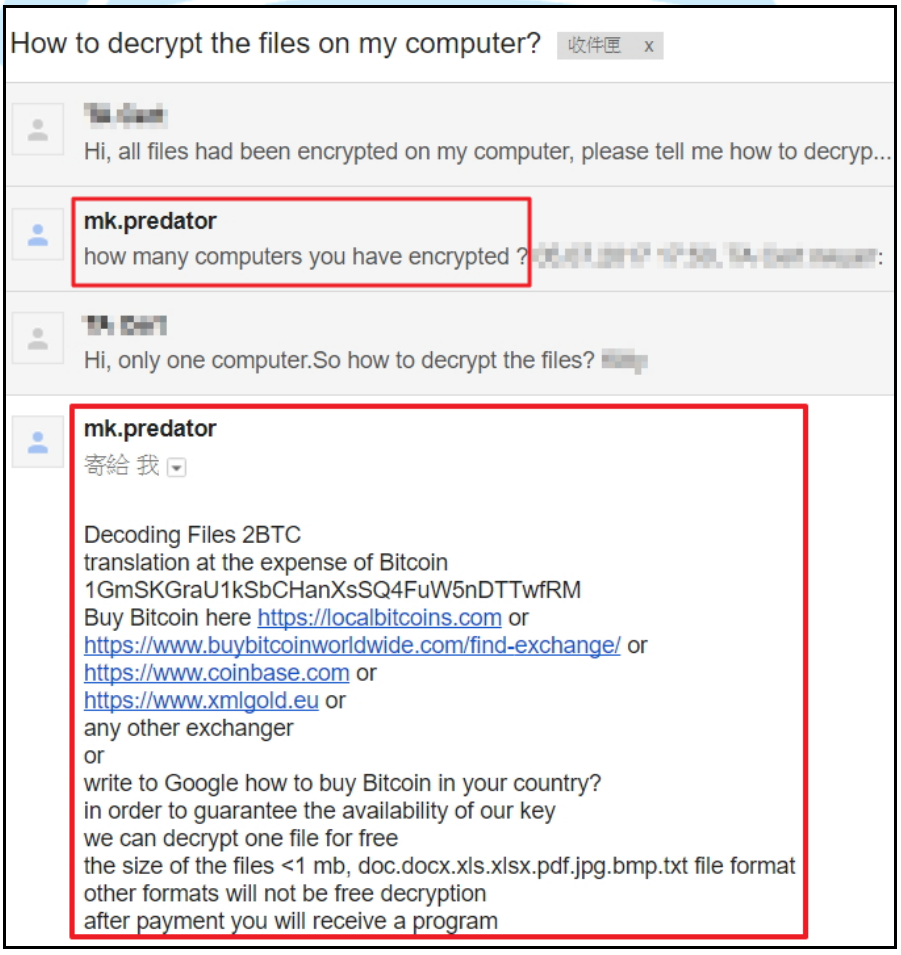
Message	Generated	Username
遠端桌面服務: 工作階段登入成功:	2017-04-28 06:46:54Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-04-28 07:03:30Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-04-28 07:08:21Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-01 06:28:18Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-04 06:09:48Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-15 02:01:32Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-15 04:51:24Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-15 05:40:19Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-24 07:51:10Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-25 08:41:38Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-25 09:43:52Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-28 07:38:41Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-29 19:35:35Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-30 15:38:02Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-30 19:16:40Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-31 08:18:18Z	NT AUTHORITY\SYSTEM
遠端桌面服務: 工作階段登入成功:	2017-05-31 08:34:05Z	NT AUTHORITY\SYSTEM

Message	Generated	
遠端桌面服務: 使用者驗證成功:	2017-06-07 18:23:33Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 18:31:52Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 18:54:15Z	使用者: administrator 來源網路位址: 162.209.168.91
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:02:28Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:21:55Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:22:09Z	使用者: administrator 來源網路位址: 58.218.213.25
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:22:39Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:24:48Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:33:01Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 19:55:12Z	使用者: administrator 來源網路位址: 162.209.168.91
遠端桌面服務: 使用者驗證成功:	2017-06-07 20:03:21Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 20:25:28Z	
遠端桌面服務: 使用者驗證成功:	2017-06-07 20:33:35Z	

11. 在###DECRYPT MY FILES###的文字檔中，在贖金部分沒有說明為了獲得 Nemesis 解密器應該支付多少錢。相反地，它建議寫信到罪犯的電子郵件信箱(mk.predator@aol.com 或 mk.predator@inbox.lv)來獲取說明，此勒索手法與 Cry36 病毒特徵相同。

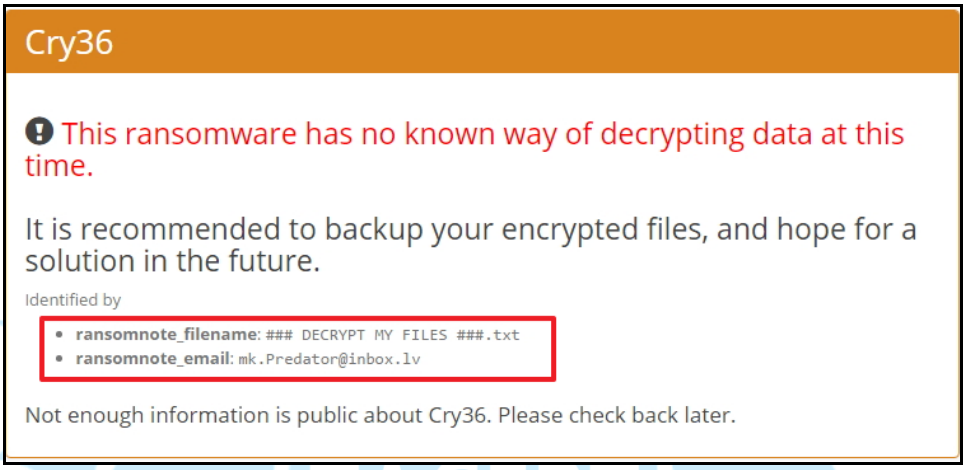


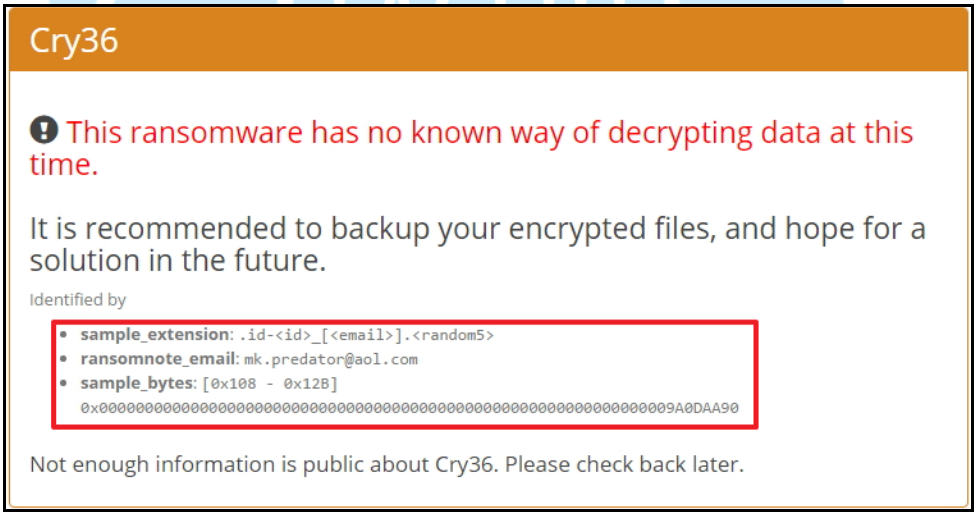
12. 為了瞭解 mk.predator@aol.com 與 mk.predator@inbox.lv 兩個信箱是否還活動著，故寄信給到上列兩個信箱，並隨信附上 personal ID，其中 mk.predator@aol.com 信箱馬上收到駭客回信，詢問有多少台電腦被加密，並且告知受害者要付 2 個比特幣(約台幣 12 萬元)與付款方式，駭客也告訴受害者為了確認解密的 key 是有效的，可以免費解密一個檔案。另外，從駭客回信的 Mail 中，發現到其來源 IP:85.15.103.238 為來自俄羅斯的 IP。



```
Received: from [192.168.0.105] (a85-15-103-238.pppoe.vtelecom.ru
[85.15.103.238]) (using TLSv1 with cipher DHE-RSA-AES128-SHA
(128/128 bits)) (No client certificate requested) by mtaout-
aam01.mx.aol.com (MUA/Third Party Client Interface) with ESMTPSA
id B1C3438000089 for <[redacted]@[redacted]>; [redacted]
```

13. 將###DECRYPT MY FILES###文字檔與被加密的檔案上傳至勒索病毒辨別網站(https://id-ransomware.malwarehunterteam.com)，檢測結果為 Cry36 勒索病毒。

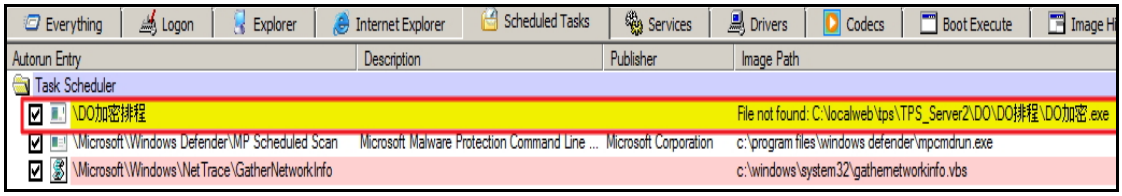




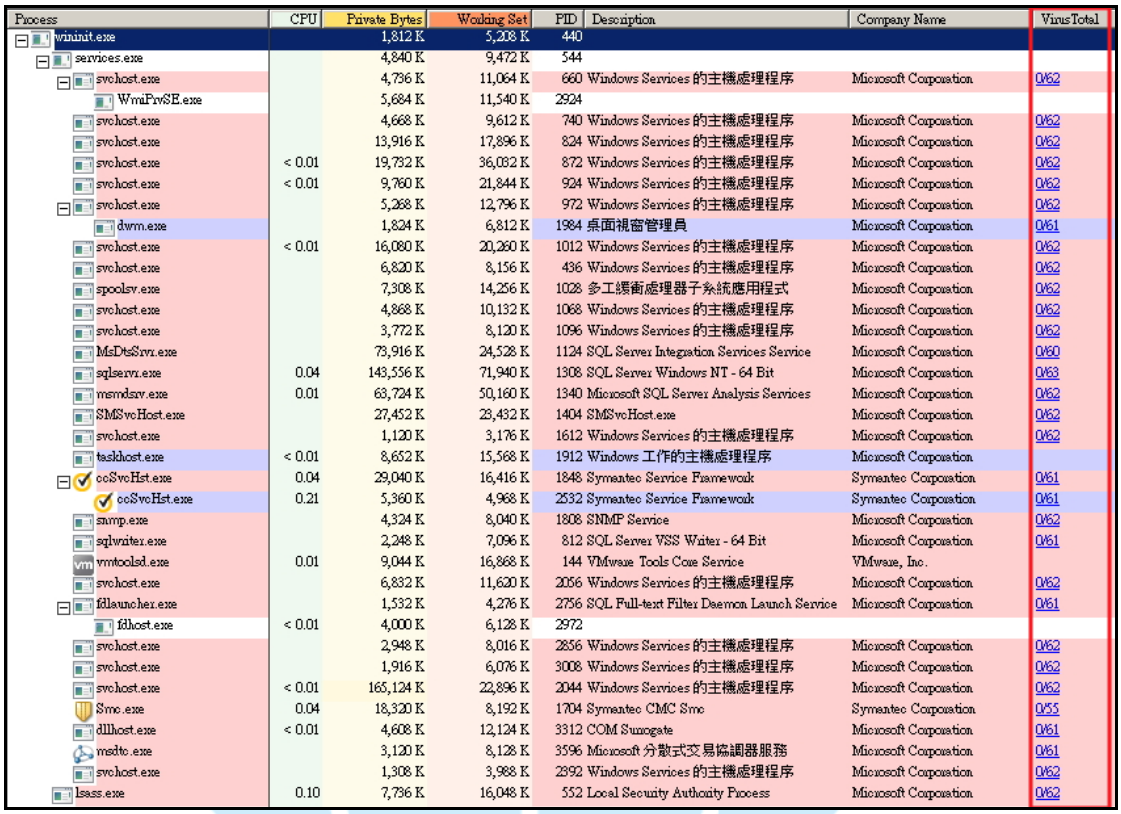
14. 在下載資料夾內，發現一個可疑執行檔 svchost.exe，其建立日期與修改日期皆為 106 年 6 月 8 日上午 5:10，與主機內檔案被加密的時間相同。將 svchost.exe 上傳至 virustotal 檢測，其為惡意程式的比率 5/61，雖然不高但有 5 家防毒公司認為其為木馬程式。另外，svchost.exe 為 Windows 系統中常用的服務啟動程序之執行檔，它只能提供條件讓其他服務在這裡被啟動，而它自己本身卻不能給使用者提供任何服務，通常位

於 ”Windows\system32” 目錄下，在此受測主機內卻在下載資料夾中，推測可能曾被駭客用來啟動某種的服務程序。

15. 透過 Autoruns 工具檢視，發現在 C:\windows\syswow64\drivers\資料夾中有 9 個驅動程式的系統檔案遺失，遺失的檔案有 amdide.sys、brfiltup.sys、errdev.sys、hidbatt.sys、qd260x64.sys、ipmidrv.sys、lsi_scsi.sys、peauth.sys 與 sfloppy.sys。此外，也發現下列 4 個檔案遺失，分別是 C:\windows\syswow64\scext.dll、C:\windwos\syswow64\ie4unit.exe、C:\localweb\tps\TPS_server2\DO\DO 排程\DO 加密.exe 與 C:\Program Files(x86)\Common Files\Symantec Shared\EENGINE\cc.SvcHst.exe /hccCommon，其中在 Task Scheduler 項目中之「C:\localweb\tps\TPS_server2\DO\DO 排程\DO 加密.exe」非一般常見檔案，推測可能為駭客所用執行檔。

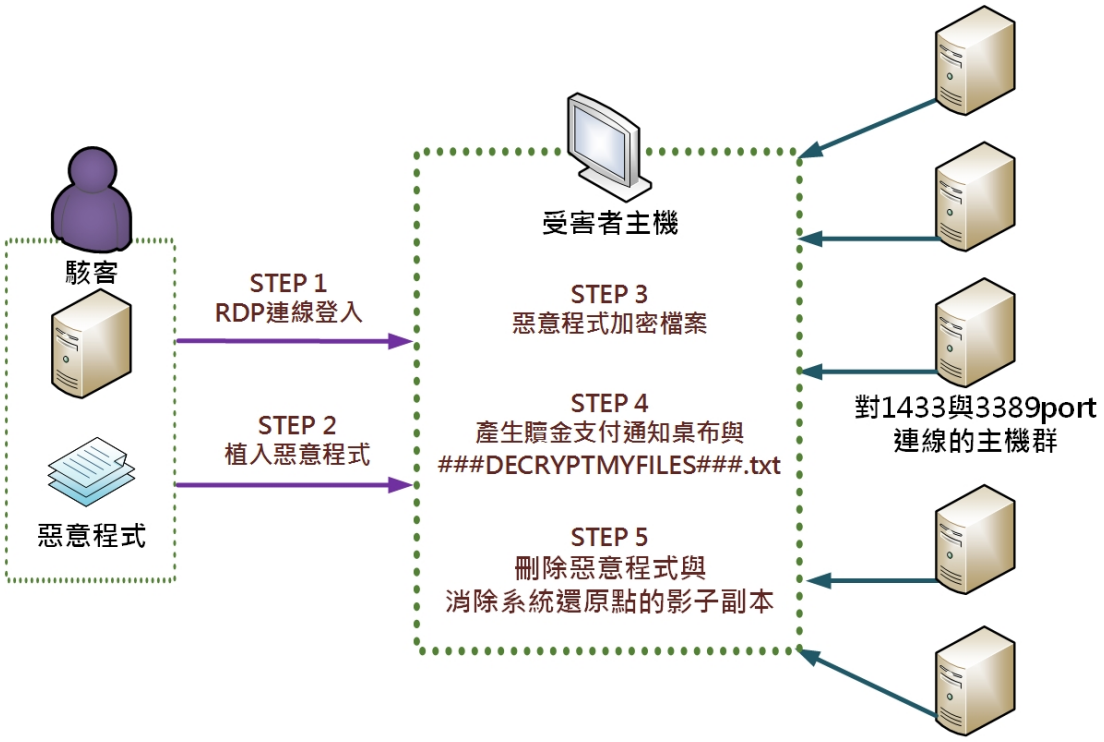


16. 使用 Process Explorer 觀察是否有惡意程式執行中，但無法找到惡意程式活動狀態，又使用惡意程式檢測軟體掃描整台受測主機也無法掃出惡意程式，推測可能在駭客執行完加密程序後就將惡意程式刪除。



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
wininit.exe		1,812 K	5,208 K	440			
services.exe		4,840 K	9,472 K	544			
svchost.exe		4,736 K	11,064 K	660	Windows Services 的主機處理程序	Microsoft Corporation	0/62
WmiPrvSE.exe		5,684 K	11,540 K	2924			
svchost.exe		4,668 K	9,612 K	740	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe		13,916 K	17,896 K	824	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe	< 0.01	19,732 K	36,032 K	872	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe	< 0.01	9,760 K	21,844 K	924	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe		5,268 K	12,796 K	972	Windows Services 的主機處理程序	Microsoft Corporation	0/62
dwm.exe		1,824 K	6,812 K	1984	桌面視窗管理員	Microsoft Corporation	0/61
svchost.exe	< 0.01	16,080 K	20,260 K	1012	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe		6,820 K	8,156 K	436	Windows Services 的主機處理程序	Microsoft Corporation	0/62
spoolsv.exe		7,308 K	14,256 K	1028	多工緩衝處理器子系統應用程式	Microsoft Corporation	0/62
svchost.exe		4,868 K	10,132 K	1068	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe		3,772 K	8,120 K	1096	Windows Services 的主機處理程序	Microsoft Corporation	0/62
MsDtsSrvr.exe		73,916 K	24,528 K	1124	SQL Server Integration Services Service	Microsoft Corporation	0/60
sqlservr.exe	0.04	143,556 K	71,940 K	1308	SQL Server Windows NT - 64 Bit	Microsoft Corporation	0/63
msmdsrv.exe	0.01	63,724 K	50,160 K	1340	Microsoft SQL Server Analysis Services	Microsoft Corporation	0/62
SMSvcHost.exe		27,452 K	23,432 K	1404	SMSvcHost.exe	Microsoft Corporation	0/62
svchost.exe		1,120 K	3,176 K	1612	Windows Services 的主機處理程序	Microsoft Corporation	0/62
taskhost.exe	< 0.01	8,652 K	15,568 K	1912	Windows 工作的主機處理程序	Microsoft Corporation	
ccSvcHst.exe	0.04	29,040 K	16,416 K	1848	Symantec Service Framework	Symantec Corporation	0/61
ccSvcHst.exe	0.21	5,360 K	4,968 K	2532	Symantec Service Framework	Symantec Corporation	0/61
snmp.exe		4,324 K	8,040 K	1808	SNMP Service	Microsoft Corporation	0/62
sqlwriter.exe		2,248 K	7,096 K	812	SQL Server VSS Writer - 64 Bit	Microsoft Corporation	0/61
vmtoolsd.exe	0.01	9,044 K	16,868 K	144	VMware Tools Core Service	VMware, Inc.	
svchost.exe		6,832 K	11,620 K	2056	Windows Services 的主機處理程序	Microsoft Corporation	0/62
fdlauncher.exe		1,532 K	4,276 K	2756	SQL Full-text Filter Daemon Launch Service	Microsoft Corporation	0/61
fdhost.exe	< 0.01	4,000 K	6,128 K	2972			
svchost.exe		2,948 K	8,016 K	2856	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe		1,916 K	6,076 K	3008	Windows Services 的主機處理程序	Microsoft Corporation	0/62
svchost.exe	< 0.01	165,124 K	22,896 K	2044	Windows Services 的主機處理程序	Microsoft Corporation	0/62
Smc.exe	0.04	18,320 K	8,192 K	1704	Symantec CMC Smc	Symantec Corporation	0/55
dllhost.exe	< 0.01	4,608 K	12,124 K	3312	COM Surrogate	Microsoft Corporation	0/61
msdtc.exe		3,120 K	8,128 K	3596	Microsoft 分散式交易協調器服務	Microsoft Corporation	0/61
svchost.exe		1,308 K	3,988 K	2892	Windows Services 的主機處理程序	Microsoft Corporation	0/62
lsass.exe	0.10	7,736 K	16,048 K	552	Local Security Authority Process	Microsoft Corporation	0/62

III.網路架構圖



1. 駭客透過 RDP 方式登入系統。
2. 植入惡意程式於受害主機。
3. 惡意程式掃描系統，並用兩種加密演算法對受害主機內所有文件進行加密。
4. 加密完成後置換使用者桌布，並在每個資料夾中產生一個 ###DECRYPTMYFILES###.txt 文字檔。
5. 刪除惡意程式與消除系統還原點的影子副本。

IV.建議與總結

1. 經檢測結果判斷本受測主機感染 Cry36 勒索病毒，通常 Cry36 病毒滲透入主機後，會掃描所有本機內磁碟機、在網路上分享的磁碟機與其他連接主機的外接記憶體裝置，之後對電腦內所有文件進行加密，雖然 Cry36 的加密方式複雜，但不會損壞、移動或刪除文件。

2. 由於 Cry36 病毒會消除系統還原點的影子副本，加上加密是使用兩種加密演算法對電腦內檔案加密，所以沒有私鑰基本上是無法救回檔案。
3. 目前尚無有效的解密程式可將被加密的檔案還原，為有效預防感染 Cry36 勒索病毒，建議使用者定期做好重要資料備份作業。
4. 本受測主機對外開啟 11 個連接埠，容易使主機變成駭客攻擊入侵的對象，建議管理者檢視這些連接埠開啟的必要性。
5. 本案受測主機被駭客以 RDP 方式侵入，建議加強密碼強度，設定含英文及數字組合之 8 位以上的密碼，並定期變更密碼。
6. 檢測時發現該受測主機之防火牆功能未啟動，建議管理者重新檢視防火牆設定。