

個案分析-

具自我摧毀功能的
無檔案式勒索病毒
Sorebrect(aes_ni_0day)
事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

106年8月

I. 事件簡介

1. 近幾年加密勒索病毒盛行，陸續出現的病毒種類與版本琳瑯滿目，台灣深受其害的電腦不計其數，影響範圍從小至個人電腦，大至各行各業的伺服器。
2. 除了一般使用者與企業會遭受勒索病毒攻擊外，政府單位或學術單位也成為勒索病毒的攻擊對象。
3. 此類勒索病毒的共同點都是加密電腦內檔案與要求使用者以比特幣支付贖金，因為比特幣具匿名且可規避金流追查的特性，深深受犯罪組織的喜愛。
4. 本單位近期取得「具自我摧毀功能的無檔案式勒索病毒」樣本進行研究分析，此版本病毒有別於以往的勒索病毒，感染後病毒本身即自我毀滅，增加樣本取得的困難性。

II. 事件檢測

1. 使用 2 台安裝 Windows 7 系統的 VM 虛擬主機進行隔離環境測試，兩台主機分別為「已感染的 ABC 主機」(IP:140. X. X. 43)與「待感染的 DEF 主機」(IP:140. X. X. 44)，惡意程式樣本名稱為 virus.exe 的執行檔，將程式 virus.exe 放於 ABC 主機上執行。



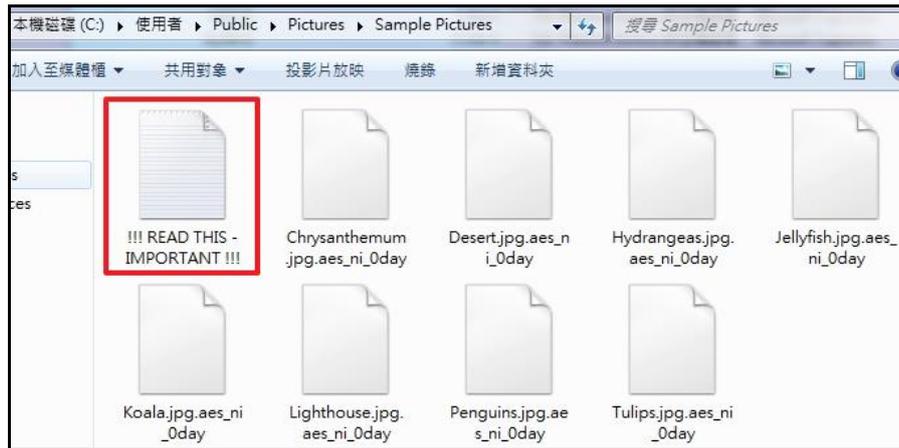
2. 為了觀察惡意程式在網路上的擴散情形，故在 DEF 主機上設置一些網路共用的資料夾，並且在 ABC 主機上設置一個連到 DEF 主機之共享資料夾的網路磁碟機(代號為 Z)。



3. 程式 virus.exe 執行後，該程式原始檔便會自我移除，讓使用者無法再次取得程式的樣本，如同加密勒索軟體般有自我銷毀機制。之後開始針對主機內部檔案進行加密。



4. 當主機內的檔案被加密後，在資料夾中會出現!!! READ THIS - IMPORTANT !!! .txt 文字檔，通知受害者你的文件和其他檔案都已經被加密，也發現網路磁碟機 Z 中的檔案也被加密。

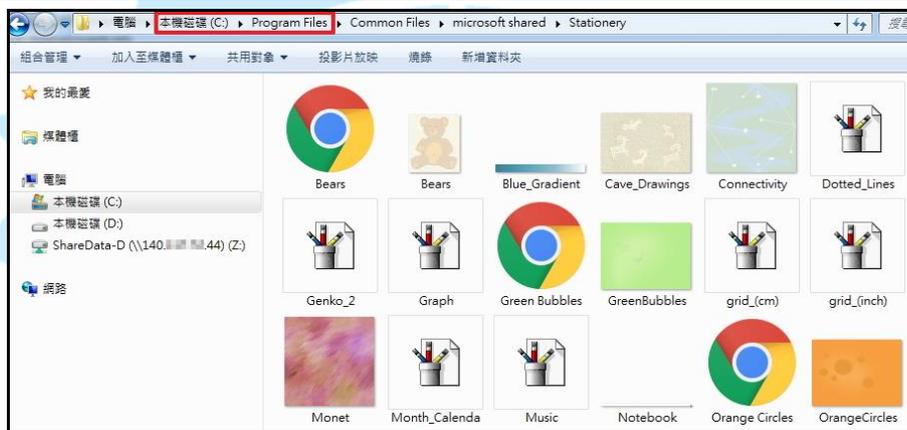
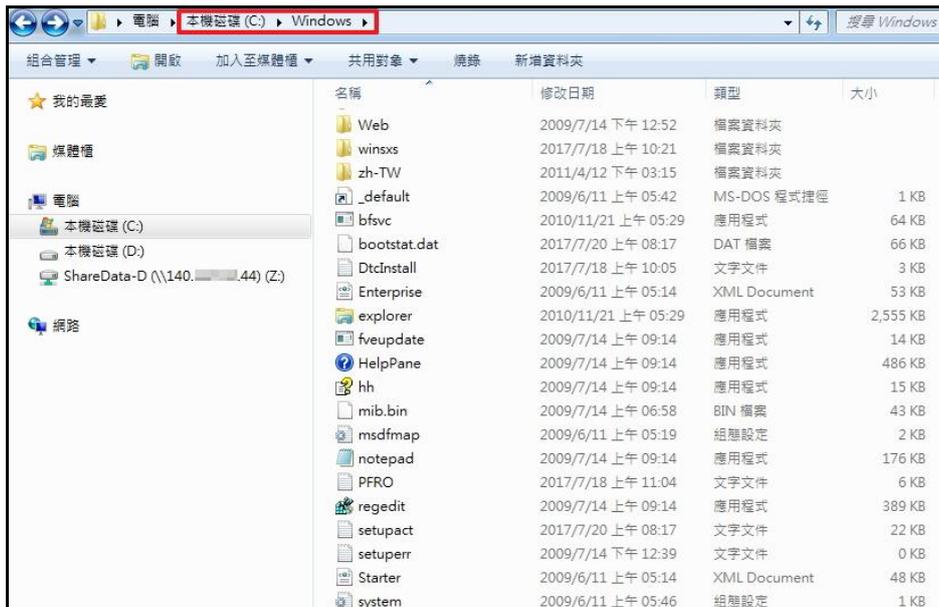


名稱	修改日期	類型	大小
!!! READ THIS - IMPORTANT !!!	2017/7/18 上午 10:42	文字文件	3 KB
DEF-PC.arn.aes_ni_0day	2017/7/18 上午 11:53	AES_NI_0DAY 檔案	5,097 KB
DEF-PC.txt.aes_ni_0day	2017/7/18 上午 11:53	AES_NI_0DAY 檔案	27 KB

5. 檢查所有資料夾發現被加密的檔案其檔案名稱都變為「原檔案名稱.aes_ni_0day」，也發現.exe、.dll、.lnk與.sys等檔案類型的檔案沒有被加密，而且若檔案大小太小也不會被加密。

名稱	類型	大小	修改日期
!!! READ THIS - IMPORTANT !!!	文字文件	3 KB	2017/7/18 上午 10:36
Desert.jpg.aes_ni_0day	AES_NI_0DAY 檔案	827 KB	2009/7/14 下午 12:52
Eula.txt.aes_ni_0day	AES_NI_0DAY 檔案	8 KB	2017/5/31 上午 10:54
Google Chrome	捷徑	3 KB	2017/7/18 上午 10:31
NTUSER.DAT	文字文件	1 KB	2011/4/12 下午 03:23
NTUSER.DAT.LOG1.aes_ni_0day	AES_NI_0DAY 檔案	194 KB	2017/7/18 上午 10:05
NTUSER.DAT.LOG2	LOG2 檔案	0 KB	2009/7/14 上午 10:03
Sleep Away.mp3.aes_ni_0day	AES_NI_0DAY 檔案	4,730 KB	2009/7/14 下午 12:52
Tcpvcon	應用程式	195 KB	2017/5/31 上午 10:54
tcpview.chm.aes_ni_0day	AES_NI_0DAY 檔案	41 KB	2017/5/31 上午 10:54
Tcpview	應用程式	294 KB	2017/5/31 上午 10:54
TCPVIEW.HLP.aes_ni_0day	AES_NI_0DAY 檔案	9 KB	2017/5/31 上午 10:54
twain_32.dll	應用程式擴充	50 KB	2010/11/21 上午 05:29
VirusSample.zip.aes_ni_0day	AES_NI_0DAY 檔案	1,421 KB	2017/6/29 上午 11:27
vm3dmp.sys	系統檔案	220 KB	2013/8/26 下午 01:10
Wildlife.wmv.aes_ni_0day	AES_NI_0DAY 檔案	25,632 KB	2009/7/14 下午 12:52
Windows PowerShell Modules	捷徑	3 KB	2009/6/11 上午 05:24

6. 檢視整台 ABC 主機發現在 C:\Windows 與 ProgramFiles 這兩個資料夾中的所有檔案都沒有被加密，可見此病毒並非加密所有資料夾中的檔案。



7. 檢視背景執行中的程式發現，程式 virus.exe 執行後，會呼叫程式 svchost.exe，之後 svchost.exe 執行時會呼叫程式 vssadmin.exe 與 timeout.exe，而 timeout.exe 執行後會執行程式 bcdedit.exe 與 wevtutil.exe。從這些程式執行的蹤跡發現 svchost.exe 一直持續執行著，而程式 vssadmin.exe 執行後會刪除系統內的影子副本，timeout.exe 執行後會暫停命令處理器 10 秒鐘，wevtutil.exe 執行時會先列出所有事件紀錄，之後再將它們陸續清除。

Process	D	Image Path	Life Time	Command
virus.exe (3624)		D:\VirusSample\virus.exe		"D:\VirusSample\virus.exe"
svchost.exe (3924)		W...C:\Windows\system32\svchost.exe		"C:\Windows\system32\svchost.exe"
vssadmin.exe (2980)		適...C:\Windows\system32\vssadmin.exe		C:\Windows\system32\vssadmin.exe Delete Shadows /All
cmd.exe (2284)		W...C:\Windows\system32\cmd.exe		cmd /c ""C:\Users\ABC\AppData\Local\Temp\4666.tmp.bat"
timeout.exe (3452)		ti...C:\Windows\system32\timeout.exe		timeout /T 10
cmd.exe (2304)		W...C:\Windows\system32\cmd.exe		C:\Windows\system32\cmd.exe /c bcdedit
bcdedit.exe (964)		開...C:\Windows\system32\bcdedit.exe		bcdedit
cmd.exe (3388)		W...C:\Windows\system32\cmd.exe		C:\Windows\system32\cmd.exe /c wevtutil.exe el
wevtutil.exe (992)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe el
wevtutil.exe (2288)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "Analytic"
wevtutil.exe (3344)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "Application"
wevtutil.exe (3060)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "DirectShowFilterGraph"
wevtutil.exe (356)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "DirectShowPluginControl"
wevtutil.exe (1372)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "EndpointMapper"
wevtutil.exe (2036)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "ForwardedEvents"
wevtutil.exe (2472)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "HardwareEvents"
wevtutil.exe (3664)		E...C:\Windows\system32\wevtutil.exe		wevtutil.exe cl "Internet Explorer"

8. 檢視程式 svchost.exe 的屬性，發現程式執行時會對同一網域的電腦進行 TCP 139 port 的攻擊連線，該 port 主要應用於文件共享與列印方面，可見該病毒會掃描網域中的共用資料夾或周邊列印裝置。

Proto...	Local Address	Remote Address	State
TCP	127.0.0.1:49157	127.0.0.1:49158	ESTABLISHED
TCP	127.0.0.1:49158	127.0.0.1:49157	ESTABLISHED
TCP	140. . . .43:49298	140. . . .129:139	SYN_SENT
TCP	140. . . .43:49294	140. . . .130:139	SYN_SENT
TCP	140. . . .43:49295	140. . . .131:139	SYN_SENT
TCP	140. . . .43:49296	140. . . .132:139	SYN_SENT
TCP	140. . . .43:49297	140. . . .133:139	SYN_SENT
TCP	140. . . .43:49298	140. . . .134:139	SYN_SENT
TCP	140. . . .43:49299	140. . . .135:139	SYN_SENT
TCP	140. . . .43:49300	140. . . .136:139	SYN_SENT
TCP	140. . . .43:49301	140. . . .137:139	SYN_SENT
TCP	140. . . .43:49302	140. . . .138:139	SYN_SENT
TCP	140. . . .43:49303	140. . . .139:139	SYN_SENT
TCP	140. . . .43:49304	140. . . .140:139	SYN_SENT
TCP	140. . . .43:49305	140. . . .141:139	SYN_SENT
TCP	140. . . .43:49306	140. . . .142:139	SYN_SENT
TCP	140. . . .43:49307	140. . . .143:139	SYN_SENT
TCP	140. . . .43:49308	140. . . .144:139	SYN_SENT
TCP	140. . . .43:49309	140. . . .145:139	SYN_SENT
TCP	140. . . .43:49310	140. . . .146:139	SYN_SENT
TCP	140. . . .43:49311	140. . . .147:139	SYN_SENT
TCP	140. . . .43:49312	140. . . .148:139	SYN_SENT
TCP	140. . . .43:49313	140. . . .149:139	SYN_SENT
TCP	140. . . .43:49314	140. . . .150:139	SYN_SENT
TCP	140. . . .43:49315	140. . . .151:139	SYN_SENT
TCP	140. . . .43:49316	140. . . .152:139	SYN_SENT
TCP	140. . . .43:49317	140. . . .153:139	SYN_SENT
TCP	140. . . .43:49318	140. . . .154:139	SYN_SENT
TCP	140. . . .43:49319	140. . . .155:139	SYN_SENT
TCP	140. . . .43:49320	140. . . .156:139	SYN_SENT
TCP	140. . . .43:49321	140. . . .157:139	SYN_SENT
TCP	140. . . .43:49322	140. . . .158:139	SYN_SENT
TCP	140. . . .43:49323	140. . . .159:139	SYN_SENT

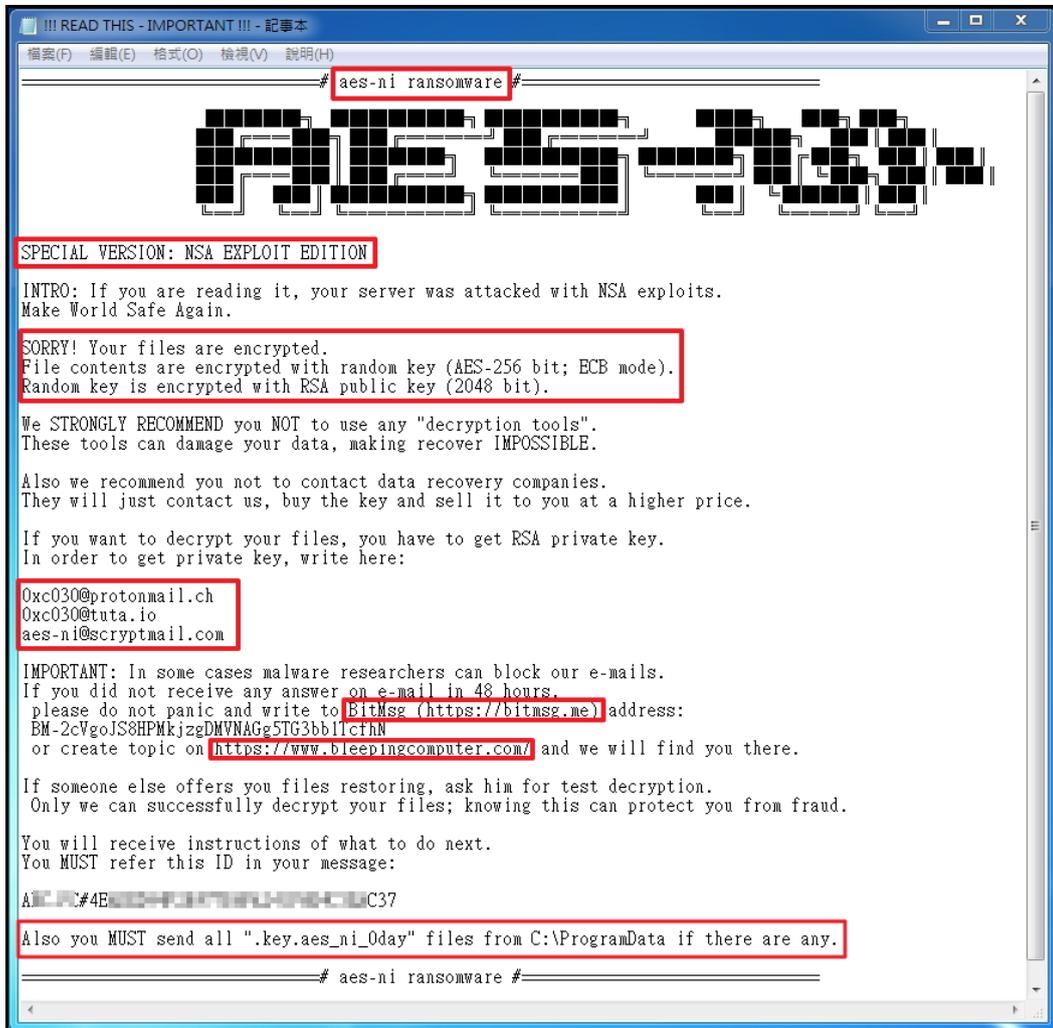
9. 從截錄的封包內容檢視，觀察到惡意程式 virus.exe 執行後，會對內部網路進行 139 port (netbios-ssn) 與 445 port 的掃描，並嘗試針對能夠存取的共享資料夾進行加密，若有連接網路磁碟機或 NAS 就有可能所儲存的檔案遭受到破壞。

Time	Service	Size	Events	Displaying 1 - 20 of 326
2017-Jul-20 11:47:44	IP / TCP / OTHER	414 B	140.111.1.43 -> 140.111.1.39	50330 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.18	49239 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.19	49240 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.20	49241 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.41	49262 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	354 B	140.111.1.43 -> 140.111.1.35	49256 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.3	49224 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	354 B	140.111.1.43 -> 140.111.1.39	49260 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.38	49259 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.33	49254 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.40	49261 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	354 B	140.111.1.43 -> 140.111.1.32	49253 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.31	49252 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.2	49223 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.30	49251 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	194 B	140.111.1.43 -> 140.111.1.53	49274 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.16	49237 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.7	49228 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.17	49238 -> 139 (netbios-ssn)
2017-Jul-20 09:59:20	IP / TCP / OTHER	374 B	140.111.1.43 -> 140.111.1.81	49302 -> 139 (netbios-ssn)

Time	Service	Size	Events	Displaying 1 - 20 of 136
2017-Jul-20 10:00:03	IP / TCP / SMB	2.34 KB	140.111.1.43 -> 140.111.1.35	49476 -> 445 (cifs)
2017-Jul-20 10:00:03	IP / TCP / SMB	1.91 KB	140.111.1.43 -> 140.111.1.35	49477 -> 445 (cifs)
2017-Jul-20 10:00:03	IP / TCP / SMB	1.91 KB	140.111.1.43 -> 140.111.1.35	49478 -> 445 (cifs)
2017-Jul-20 10:00:03	IP / TCP / SMB	7.72 KB	140.111.1.43 -> 140.111.1.39	49479 -> 445 (cifs)
2017-Jul-20 10:03:16	IP / TCP / SMB	2.27 KB	140.111.1.43 -> 140.111.1.174	49518 -> 445 (cifs)
2017-Jul-20 10:03:16	IP / TCP / SMB	1.84 KB	140.111.1.43 -> 140.111.1.174	49519 -> 445 (cifs)
2017-Jul-20 10:03:16	IP / TCP / SMB	1.84 KB	140.111.1.43 -> 140.111.1.174	49520 -> 445 (cifs)
2017-Jul-20 10:03:17	IP / TCP / SMB	2.27 KB	140.111.1.43 -> 140.111.1.208	49522 -> 445 (cifs)
2017-Jul-20 10:03:17	IP / TCP / SMB	1.84 KB	140.111.1.43 -> 140.111.1.208	49523 -> 445 (cifs)
2017-Jul-20 10:03:17	IP / TCP / SMB	1.84 KB	140.111.1.43 -> 140.111.1.208	49524 -> 445 (cifs)
2017-Jul-20 10:03:18	IP / TCP / SMB	2.43 KB	140.111.1.43 -> 140.111.1.229	49530 -> 445 (cifs)
2017-Jul-20 10:03:18	IP / TCP / SMB	2.00 KB	140.111.1.43 -> 140.111.1.229	49531 -> 445 (cifs)
2017-Jul-20 10:03:18	IP / TCP / SMB	2.00 KB	140.111.1.43 -> 140.111.1.229	49532 -> 445 (cifs)
2017-Jul-20 10:03:17	IP / TCP / SMB	6.04 KB	140.111.1.43 -> 140.111.1.181	49521 -> 445 (cifs)
2017-Jul-20 10:05:38	IP / TCP / SMB	2.81 KB	140.111.1.43 -> 140.111.1.82	49577 -> 445 (cifs)
2017-Jul-20 10:05:38	IP / TCP / SMB	2.24 KB	140.111.1.43 -> 140.111.1.82	49578 -> 445 (cifs)
2017-Jul-20 10:05:39	IP / TCP / SMB	2.24 KB	140.111.1.43 -> 140.111.1.82	49579 -> 445 (cifs)
2017-Jul-20 10:05:39	IP / TCP / SMB	2.33 KB	140.111.1.43 -> 140.111.1.35	49580 -> 445 (cifs)
2017-Jul-20 10:05:39	IP / TCP / SMB	1.90 KB	140.111.1.43 -> 140.111.1.35	49581 -> 445 (cifs)
2017-Jul-20 10:05:39	IP / TCP / SMB	1.90 KB	140.111.1.43 -> 140.111.1.35	49582 -> 445 (cifs)

10. 從!!!READ THIS - IMPORTANT !!! .txt 文字檔中得知該病毒名稱為 aes-ni ransomware，在文字檔開頭提到它是特別版的 NSA EXPLOIT 版，與舊版的 aes-ni 不同，主機內的檔案是使用 RSA-2048 公開金鑰加密 AES-256 亂數產生的金鑰所加密，並且警告任何嘗試用第三方的解密工具都可能毀損已被加密的檔案，必須透過購買他們的 RSA 私密金鑰才能解救這些檔案。除了提供 3 個聯絡用的電子信箱(0xc030@protomail.ch、0xc030@tuta.io 與

aes-ni@scryptmail.com)給受害者外，也告訴受害者可以透過 BitMsg 或至 bleedingcomputer 網站上開主題論壇方式聯絡，最後也告訴受害者必須寄所有在 C:\ProgramData 內檔名中有「.key.aes_ni_0day」名稱的金鑰給他們。



11. 將!!!READ THIS - IMPORTANT !!! .txt 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 AES-NI 勒索病毒。

AES-NI

⚠ This ransomware may be decryptable under certain circumstances.

Please refer to the appropriate guide for more information.

Identified by

- ransomnote_filename: !!! READ THIS - IMPORTANT !!! .txt
- ransomnote_email: aes-ni@scryptmail.com
- ransomnote_bitmessage: BM-2cVgoJS8HPmkjzgmVNVAGg5TG3bb1TcfhN
- sample_extension: .aes_ni_oday

[Click here for more information about AES-NI](#)

12. 對側錄封包內容進行分析，發現會連到一個美國 IP: 216.239.36.21 去取得憑證，並且傳送 ABC 主機的 IP 位置，該 IP 的網站名稱為 ipinfo.io，也發現另有 3 台主機與其同相同名稱，而且每次當 virus.exe 執行時，所連到的 IP 必定是這四台主機中的其中一個，可見這四個主機為駭客收集受害主機的 IP 資料用。

Timestamp	Client	Client Port	Server	Server Port	IP TTL	DNS TTL (time)	Transaction ID	Type	DNS Query	DNS Answer
2017/7/20 上午 09:54:25	140.144.43	54085	140.144.1.1	53	251	00:02:38	0xDA62	0x0001 (Host Address)	ipinfo.io	216.239.36.21
2017/7/20 上午 09:54:25	140.144.43	54085	140.144.1.1	53	251	00:02:38	0xDA62	0x0001 (Host Address)	ipinfo.io	216.239.32.21
2017/7/20 上午 09:54:25	140.144.43	54085	140.144.1.1	53	251	00:02:38	0xDA62	0x0001 (Host Address)	ipinfo.io	216.239.38.21
2017/7/20 上午 09:54:25	140.144.43	54085	140.144.1.1	53	251	00:02:38	0xDA62	0x0001 (Host Address)	ipinfo.io	216.239.34.21

216.218.206.112

- 216.239.32.21 [ipinfo.io]
- 216.239.34.21 [ipinfo.io]
- 216.239.36.21 [ipinfo.io]

IP: 216.239.36.21

- MAC: 80711FD5DC81
- NIC Vendor: Juniper Networks
- Hostname: ipinfo.io
- OS: Unknown
- TTL: 45 (distance: 19)
- Open TCP Ports: 443 (Ssl)

Sent: 9 packets (3,739 Bytes), 0.00% cleartext (0 of 0 Bytes)

216.239.36.21 [ipinfo.io] -> 140.144.43 [ABC-PC] (Windows) : 9 packets (3,739 Bytes), 0.00% cleartext (0 of 0 Bytes)

Received: 9 packets (757 Bytes), 0.00% cleartext (0 of 0 Bytes)

140.144.43 [ABC-PC] (Windows) -> 216.239.36.21 [ipinfo.io] : 9 packets (757 Bytes), 0.00% cleartext (0 of 0 Bytes)

Incoming sessions: 1

Outgoing sessions: 0

Host Details

216.239.36.21 [ipinfo.io]

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
1512	ipinfo.io.cer	cer	1 196 B	216.239.36.21 [ipinfo.io]	TCP 443	140.144.43 (Windows)	TCP 49213	TlsCertificate	2017/7/20 上午 09:54:25
1512	RapidSSL SHA256 CA - G3.cer	cer	1 065 B	216.239.36.21 [ipinfo.io]	TCP 443	140.144.43 (Windows)	TCP 49213	TlsCertificate	2017/7/20 上午 09:54:25

13. 透過 Virustotal 進行線上掃毒，該病毒檢測為惡意的比例高達 57/63，其中有 6 家防毒軟體無法檢測出此病毒，又由於此病毒與舊型的 AES-NI 病毒不同，故有少數有名的防毒公司稱此病毒為 Sorebrex 勒索病毒，像賽門鐵克

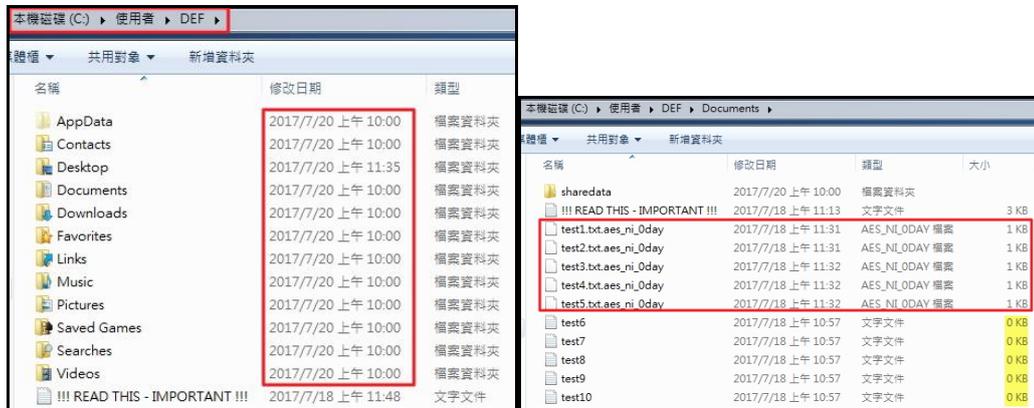
與趨勢科技這兩家公司。

SHA256:	4142ff4667f5b9986888bdc2a727db6a767f78fe1d5d4ae3346365a1d70eb76	
File name:	virus.exe	
Detection ratio:	57 / 63	
Analysis date:	2017-07-20 00:28:31 UTC (0 minutes ago)	

Antivirus	Result	Update
Ad-Aware	Trojan.AgentWDCR.LEY	20170719
AegisLab	Troj.W32.Schoolboytc	20170719
AhnLab-V3	Trojan/Win32.FileCryptor.C1922525	20170719
ALYac	Trojan.Ransom.AESNI	20170719
CAT-QuickHeal	Ransom.Sorebrect.NI5	20170719
ClamAV	Win.Ransomware.Sorebrect-6331471-0	20170719
Kaspersky	Trojan-Ransom.Win32.AecHu.c	20170719
Malwarebytes	Ransom.AESNI	20170720
Symantec	Ransom.Sorebrect	20170719
Tencent	Win32.Trojan.Inject.Auto	20170720
TrendMicro	Ransom.SOREBRECT.B	20170719
TrendMicro-HouseCall	Ransom.SOREBRECT.B	20170720
VBA32	Hoax.AecHu	20170719
VIPRE	Trojan.Win32.GenericIBT	20170720
ViRobot	Trojan.Win32.Z.Razy.1022978	20170719
Webroot	W32.Trojan.Gen	20170720
Yandex	Trojan.SchoolBoy!	20170719
Zillya	Trojan.XData.Win32.2	20170719
ZoneAlarm by Check Point	Trojan-Ransom.Win32.AecHu.c	20170719
Alibaba	☞	20170719
CMC	✔	20170719
Jiangmin	✔	20170719
Kingsoft	✔	20170720
SUPERAntiSpyware	✔	20170720
Symantec Mobile Insight	☞	20170719
TheHacker	✔	20170719
Trustlook	☞	20170720
WhiteArmor	☞	20170713
Zoner	✔	20170720

14. 檢視 DEF 主機內資料夾被感染的情形，發現除了共用資料夾與使用者 DEF 下的資料夾中檔案被加密外，其他檔案皆沒有被加密，而且在 ProgramData 資料夾內也沒有看到 RSA 金鑰，比對!!!READ THIS-IMPORTANT!!!.txt 文字

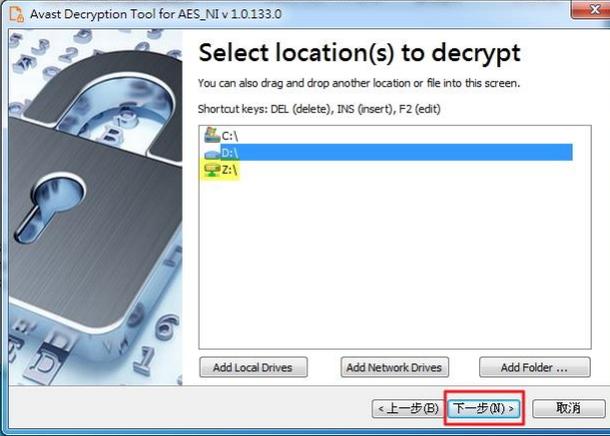
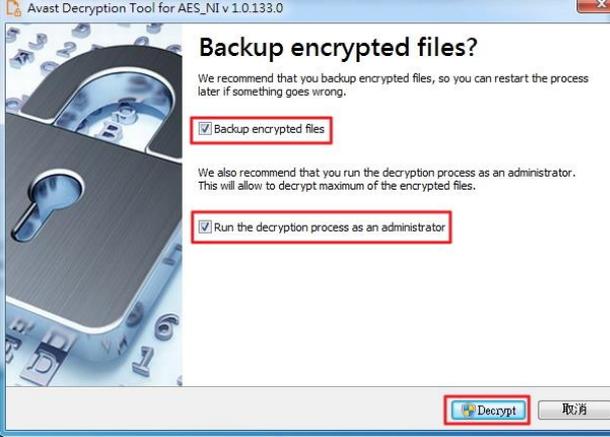
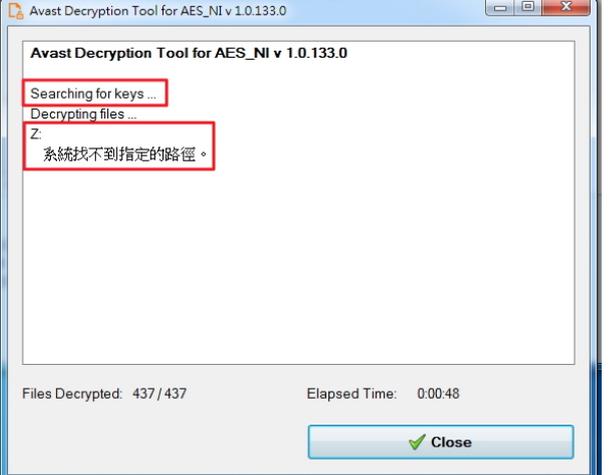
檔發現內容與 ID 都一致，可見此病毒透過區域網路散布到區域網路內的電腦時，並不會加密被感染電腦內的所有檔案，而且也沒有產生金鑰。



15. 下載 AVAST 防毒公司所提供的 AES_NI 病毒解密程式，測試是否可以將檔案解密，詳細的解密步驟如下面表格所示。

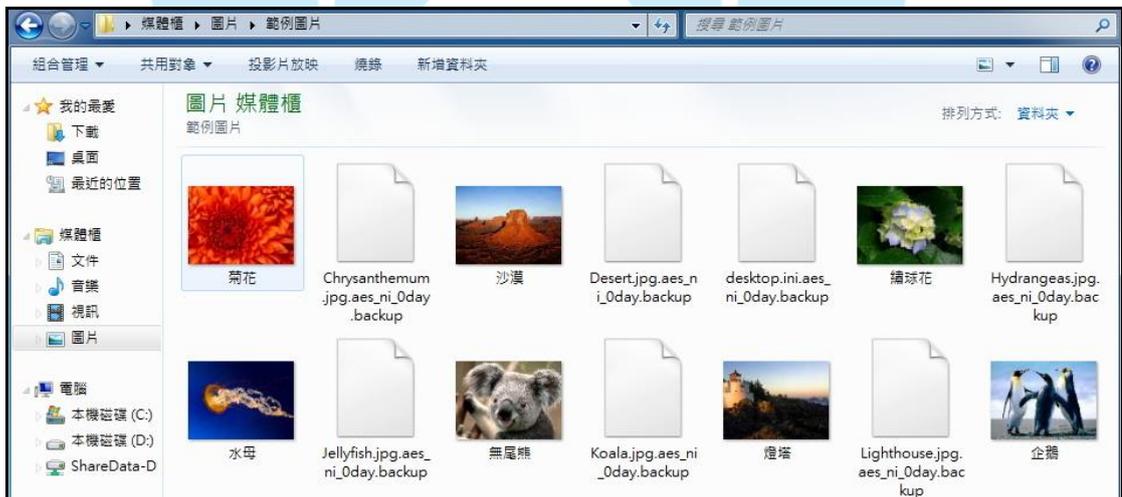


No	說明	圖示
1	執行解密程式 avast_decryptor_aes_ni , 程式視窗開啟後點選「下一步」。	

2	<p>選擇所要解密檔案的所在位置，可增加磁碟機或資料夾，確定內容後點選「下一步」。</p>	
3	<p>勾選「備分加密的檔案」與「以系統管理者權限執行解密過程」的選項，並點選「Decrypt」，開始進行檔案的解密。</p>	
4	<p>解密完成後出現 Z 磁碟機：系統找不到指定路徑的訊息，除了網路磁碟機 Z 內的檔案以外，所有檔案皆已執行解密。</p>	

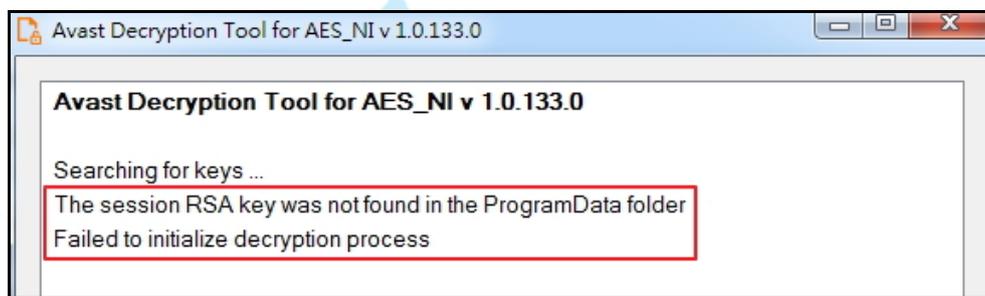
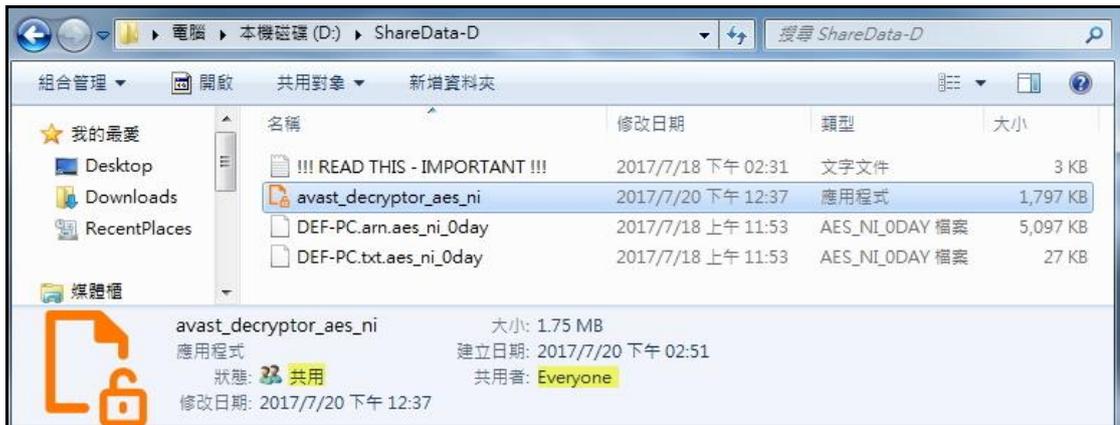
16. 執行完解密程式後，檢視系統內的檔案，發現被加密的檔案都已恢復原狀，而且在資料夾中的!!!READ THIS - IMPORTANT !!! .txt 文字檔皆已被刪除，但是網路磁碟機 Z 中的檔案仍然沒有被解密。

名稱	類型	大小	修改日期
Desert	JPEG 影像	827 KB	2009/7/14 下午 12:52
Desert.jpg.aes_ni_0day.backup	BACKUP 檔案	827 KB	2009/7/14 下午 12:52
Eula	文字文件	7 KB	2017/5/31 上午 10:54
Eula.txt.aes_ni_0day.backup	BACKUP 檔案	8 KB	2017/5/31 上午 10:54
Google Chrome	捷徑	3 KB	2017/7/18 上午 10:31
NTUSER.DAT	文字文件	1 KB	2011/4/12 下午 03:23
NTUSER.DAT.LOG1	LOG1 檔案	193 KB	2017/7/18 上午 10:05
NTUSER.DAT.LOG1.aes_ni_0day.backup	BACKUP 檔案	194 KB	2017/7/18 上午 10:05
NTUSER.DAT.LOG2	LOG2 檔案	0 KB	2009/7/14 上午 10:03
Sleep Away	MP3 格式聲音	4,730 KB	2009/7/14 下午 12:52
Sleep Away.mp3.aes_ni_0day.backup	BACKUP 檔案	4,730 KB	2009/7/14 下午 12:52
Tcpvcon	應用程式	195 KB	2017/5/31 上午 10:54
tcpview	編譯的 HTML 說明檔案	41 KB	2017/5/31 上午 10:54
tcpview.chm.aes_ni_0day.backup	BACKUP 檔案	41 KB	2017/5/31 上午 10:54
Tcpview	應用程式	294 KB	2017/5/31 上午 10:54
TCPVIEW	說明檔	8 KB	2017/5/31 上午 10:54
TCPVIEW.HLP.aes_ni_0day.backup	BACKUP 檔案	9 KB	2017/5/31 上午 10:54
twain_32.dll	應用程式擴充	50 KB	2010/11/21 上午 05:29
VirusSample	壓縮的 (zipped) 資料夾	1,420 KB	2017/6/29 上午 11:27
VirusSample.zip.aes_ni_0day.backup	BACKUP 檔案	1,421 KB	2017/6/29 上午 11:27
vm3dmp.sys	系統檔案	220 KB	2013/8/26 下午 01:10
Wildlife	Windows Media 音...	25,631 KB	2009/7/14 下午 12:52
Wildlife.wmv.aes_ni_0day.backup	BACKUP 檔案	25,632 KB	2009/7/14 下午 12:52
Windows PowerShell Modules	捷徑	3 KB	2009/6/11 上午 05:24

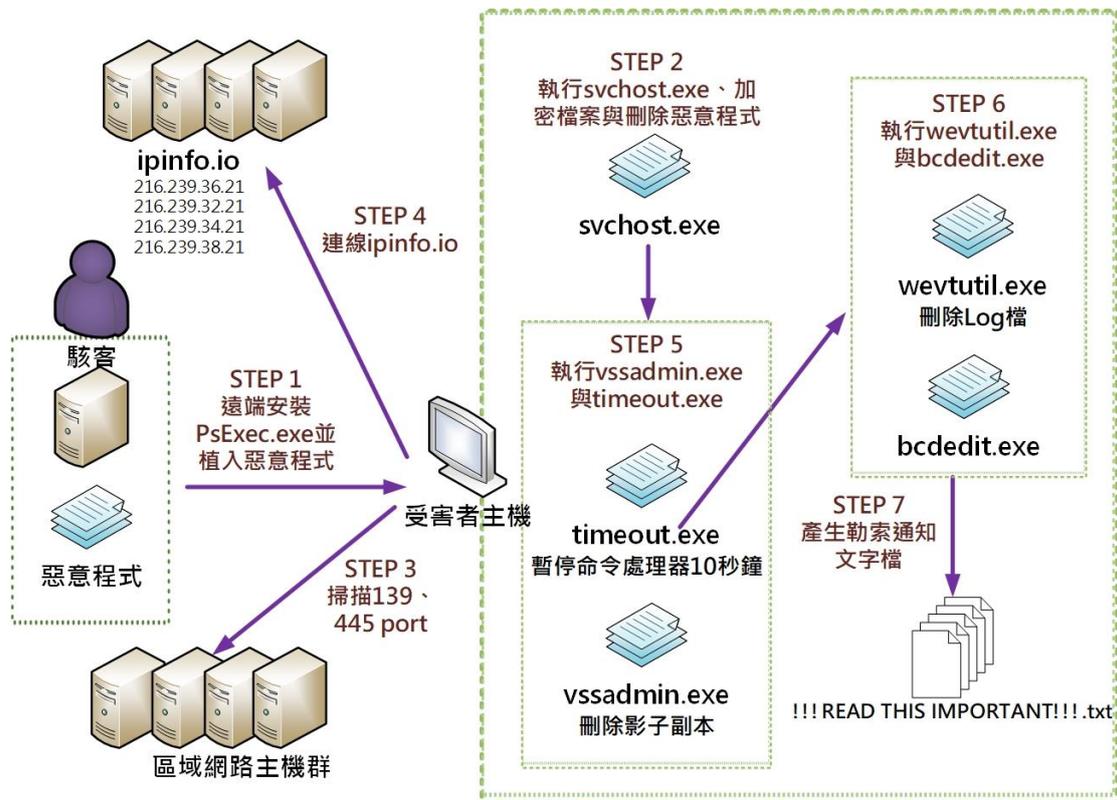


17. 將 AVAST 解密程式放入網路磁碟機 Z 中，並且至 DEF 主機上執行此解密程式，結果出現找不到金鑰的問題，將 RSA 金鑰從 ABC 主機之 ProgramData 資料夾中複製放入 DEF 主機之 ProgramData 的資料夾內，再次執行解密程式，結果成功解密，可見此解密程式一定要有病毒來源頭 ABC 主機的 RSA 金鑰才

可以將檔案解密。



III. 網路架構圖



1. 駭客從遠端安裝 PsExec.exe，並植入惡意程式於受害主機內。
2. 惡意程式執行後，呼叫程式 svchost.exe 對受害主機內檔案進行加密，並且惡意程式進行自我刪除。
3. 掃描區域網路內電腦之共用的資料夾或周邊裝置。
4. 傳送受害主機的 IP 資訊至 ipinfo.io 網站。
5. svchost.exe 執行後呼叫程式 vssadmin.exe(刪除系統還原點的影子副本)與 timeout.exe(暫停命令處理器 10 秒鐘)。
6. timeout.exe 執行後呼叫程式 bcdedit.exe 與 wevtutil.exe(清除所有事件紀錄)。
7. 加密完成後，在每個病毒拜訪過的資料夾中產生一個!!!READ THIS - IMPORTANT !!! .txt 的勒索通知文字檔。

IV. 建議與總結

為有效預防感染無檔案式勒索病毒 Sorebrect(aes_ni_0day)病毒，建議系統管理者與使用者進行下列的防禦措施：

1. 限制使用者寫入的權限：重新檢視網域中每位使用者存取網路共用資料夾的存取權限，僅提供使用者必要的存取權限，別讓任何人都能隨意存取，降低遭到勒索病毒的攻擊機會。
2. 管制 PsExec 的使用：透過 PsExec 程式可以讓管理者彈性地管理遠端主機，相對地若駭客利用它，搭配之前已預先取得的系統管理員帳號與密碼，將可在內部區域網路內安裝與執行惡意程式，因此，限制與管制一些服務與工具的使用(如 PsExec)將可以防範這些惡意程式的威脅。
3. 保持系統與網路的更新：為了避免惡意程式利用系統或網路漏洞侵入主機，建議時常執行作業系統與應用程式的更新作業。
4. 定期備份資料：通常駭客利用受害者需要重要檔案與個人資料的心理來逼迫受害者支付贖金，建議使用者平時做好資料備份作業。
5. 定期重設管理員與使用者的帳號密碼，並增加密碼強度。