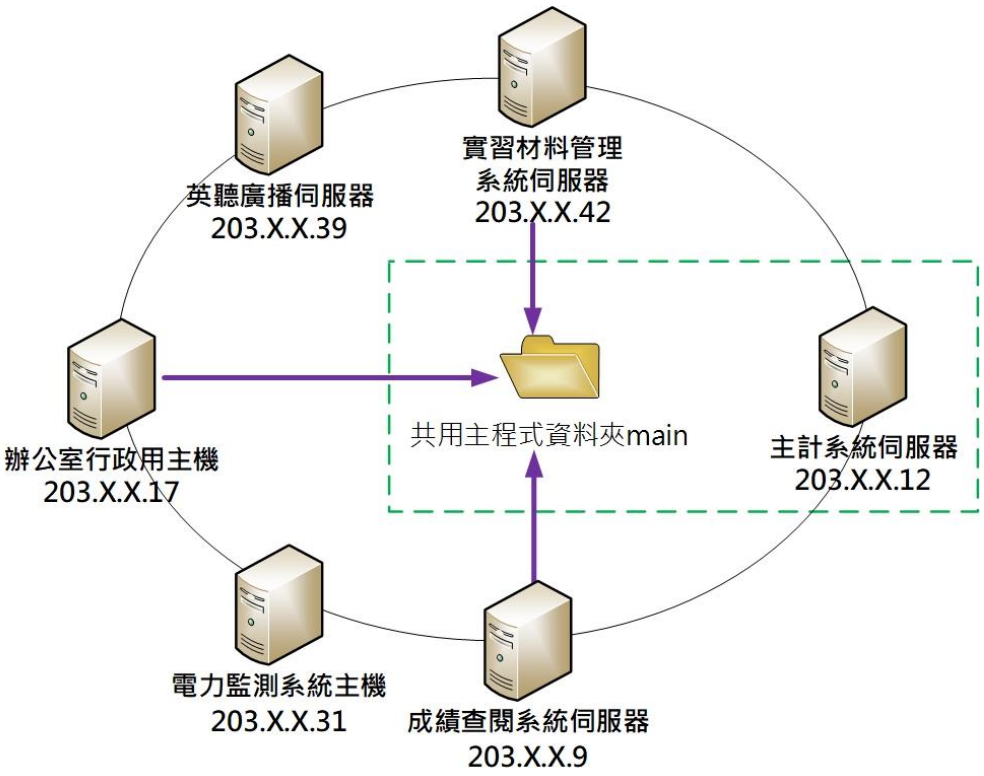
勒索病毒 Sodinokibi (REvil)
攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 10 月

一、事件簡介

1. 2019 年 9 月中旬某校發生同一區域網路內多台主機感染病毒事件，其中有三台主機連到某台主機的共用資料夾，詳細網路架構如下圖所示。



2. 該資安事件各主機感染病毒情形如下表所示，其中除了主計系統主機的共用資料夾被加密外，主計系統主機內其他資料夾都沒有被加密。

主機簡稱	IP	主機用途	系統	網路芳鄰分享(網路磁碟機)	檔案被加密的範圍
39 主機	203.X.X.39	英聽廣播伺服器	windows server 2008	---	整個主機
12 主機	203.X.X.12	主計系統	windows server 2008	主程式資料開啟網路芳鄰分享資料夾 main	除 main 資料夾內檔案被加密外，無其他檔案被加密。
42 主機	203.X.X.42	實習材料管理系統	windows server 2003	連線 12 主機的網路磁碟機	整個主機
9 主機	203.X.X.9	成績查閱系統	windows server 2008	連線 12 主機的網路磁碟機	整個主機

主機簡稱	IP	主機用途	系統	網路芳鄰分享(網路磁碟機)	檔案被加密的範圍
17 主機	203.X.X.17	辦公室行政用電腦	windows 7	連線 12 主機的網路磁碟機	整個主機
31 主機	203.X.X.31	電腦監測系統	windows 7	---	整個主機

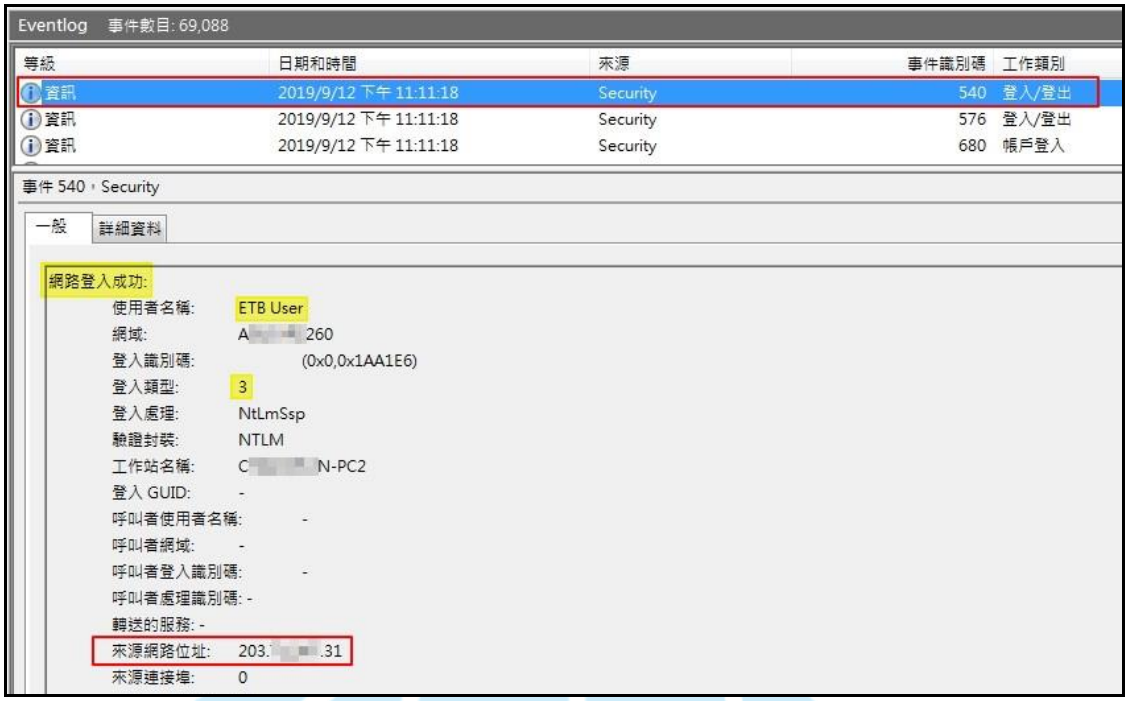
3. 部分受害主機在事件發生後即被緊急處理，無法採證，但為了解駭客在本事件之攻擊行為與危害程度，本中心對學校所能提供的多台受害主機 log 檔與電力監測系統主機進行 log 分析與鑑識作業。

二、事件檢測

1. 首先，透過分析各受害主機的事件檢視紀錄，發現這些主機大都有來自 IP:203.X.X.17 的遠端桌面登入(RDP)或網路登入的連線紀錄，而連線時間點皆介於 2019/9/12 下午 10:20 至下午 11:13 之間。

IP	事件檢視紀錄
203.X.X.39	2019/9/12 PM 10:55、PM 11:13 IP:203.X.X.17 RDP 登入
203.X.X.12	2019/9/12 PM10:55 IP:203.X.X.42 匿名登入, 2019/9/12 PM 11:11 IP:203.X.X.31 網路登入 2019/9/12 PM11:14 IP:203.X.X.9 網路登入 2019/9/12 PM 10:20 IP:203.X.X.17 網路登入
203.X.X.31	2019/9/12 PM 10:20 IP:203.X.X.17 網路登入 2019/9/12 PM 10:51、PM11:03 IP:203.X.X.17 RDP 登入 2019/9/12 PM 11:18 IBMX3550M2 主機 網路登入

其中從 12 主機的連線紀錄得知，31 主機曾在 2019/9/12 下午 11:11 以帳戶 ETB user 網路登入 12 主機。

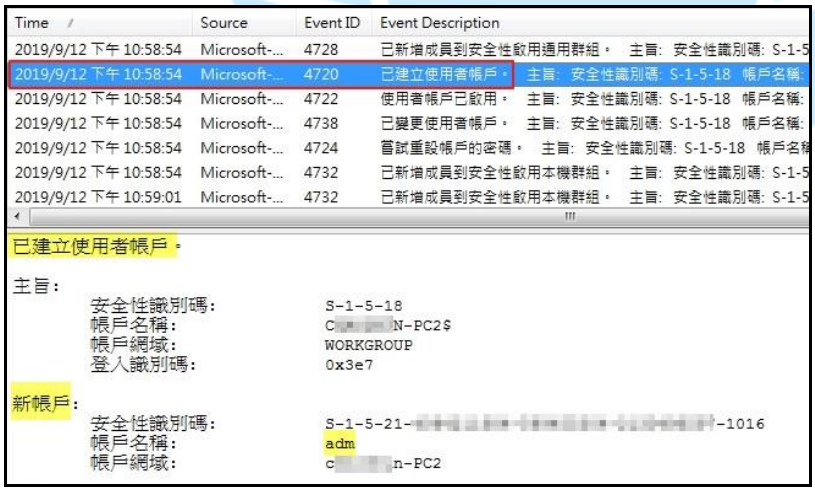


在 39 主機的連線紀錄也發現，17 主機在 2019/9/12 下午 10:55 與下午 11:13 曾經以帳戶 ETB User 登入 39 主機，這些連線所使用的登入帳戶皆為 ETB User。

A	B	C	D	E	F
稽核成功	2019/9/12 22:55	Microsoft-Windows-Security-Auditing	4624	登入	帳戶成功登入。 主旨: 安全性識別碼:SYSTEM 帳戶名稱:ETEACHER$ 帳戶網域:WORKGROUP 登入識別碼:0x3e7 登入類型:10 新登入: 安全性識別碼:ETEACHER\ETB User 帳戶名稱:ETB User 帳戶網域:ETEACHER 登入識別碼:0x800645 登入 GUID:{00000000-0000-0000-0000-000000000000} 處理程序資訊: 處理程序識別碼:0xf88 處理程序名稱:C:\Windows\System32\winlogon.exe 網路資訊: 工作站名稱:ETEACHER 來源網路位址:203. .17 來源連接埠:11904

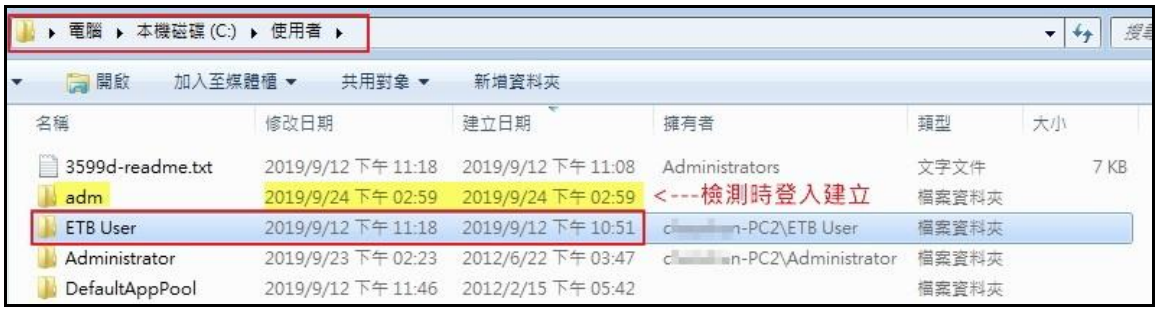
A	B	C	D	E	F
稽核成功	2019/9/12 23:13	Microsoft-Windows-Security-Auditing	4624	登入	帳戶成功登入。 主旨: 安全性識別碼:SYSTEM 帳戶名稱:ETEACHER$ 帳戶網域:WORKGROUP 登入識別碼:0x3e7 登入類型:10 新登入: 安全性識別碼:ETEACHER\ETB User 帳戶名稱:ETB User 帳戶網域:ETEACHER 登入識別碼:0x8dd328 登入 GUID:{00000000-0000-0000-0000-000000000000} 處理程序資訊: 處理程序識別碼:0xfc0 處理程序名稱:C:\Windows\System32\winlogon.exe 網路資訊: 工作站名稱:ETEACHER 來源網路位址:203.[redacted].17 來源連接埠:12237

2. 檢視 31 主機的使用者帳戶發現有一個非管理者所建立的帳戶 adm，而從事件檢視紀錄得知該帳戶 adm 於 2019/9/12 下午 10:58 被建立。

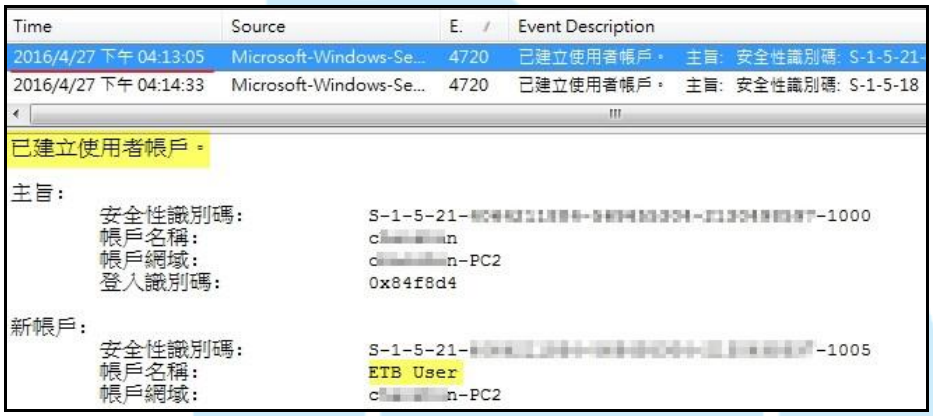


在 C:\使用者資料夾內發現一個在 2019/9/12 下午 10:51 建立的 ETB User 資料夾，但在主機登入畫面與使用者帳戶管理內無此帳戶資訊，而前述所提到帳戶

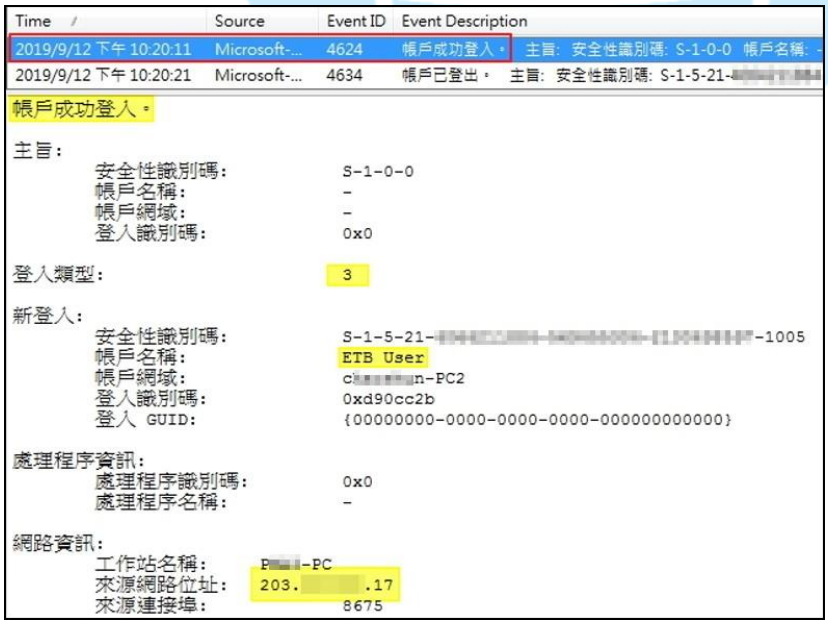
adm，則在檢測時以帳戶 adm 登入主機後才建立 adm 資料夾，可以得知駭客雖然建立 adm 帳戶，但是卻沒有使用它。

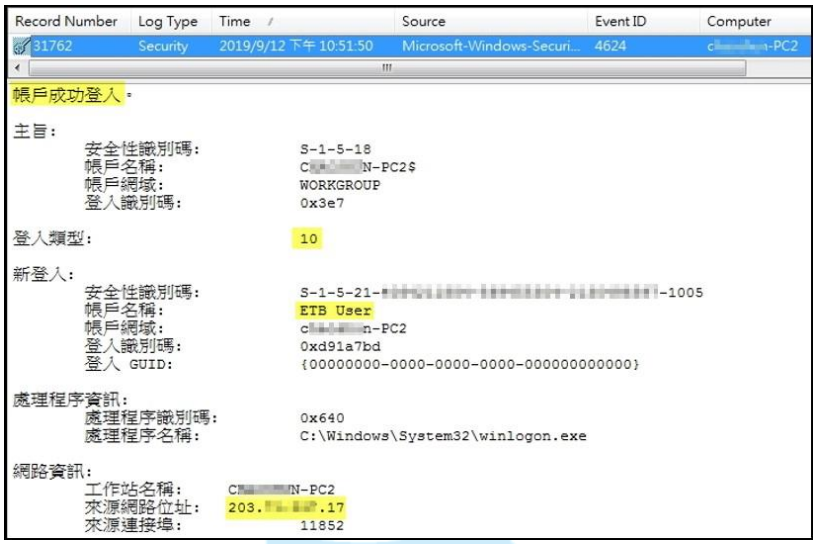


從事件檢視紀錄中得知，帳戶 ETB User 是在 2016/4/27 下午 4:13 被建立。



3. 查看 31 主機的連線紀錄，發現 9/12 下午 10:20、下午 10:51 與下午 11:03 IP:203.X.X.17 曾以帳戶 ETB User 從遠端桌面連線或以網路方式成功登入 31 主機。





Record Number	Log Type	Time	Source	Event ID	Computer
31762	Security	2019/9/12 下午 10:51:50	Microsoft-Windows-Securi...	4624	[redacted]-PC2

帳戶成功登入。

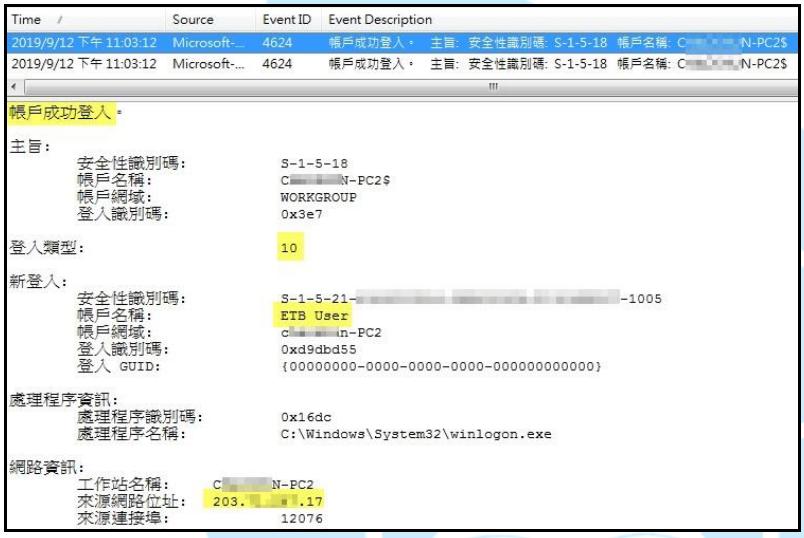
主旨:
- 安全性識別碼: S-1-5-18
- 帳戶名稱: [redacted]N-PC2$
- 帳戶網域: WORKGROUP
- 登入識別碼: 0x3e7

登入類型: 10

新登入:
- 安全性識別碼: S-1-5-21-[redacted]-1005
- 帳戶名稱: ETB User
- 帳戶網域: [redacted]n-PC2
- 登入識別碼: 0xd91a7bd
- 登入 GUID: {00000000-0000-0000-0000-000000000000}

處理程序資訊:
- 處理程序識別碼: 0x640
- 處理程序名稱: C:\Windows\System32\winlogon.exe

網路資訊:
- 工作站名稱: [redacted]N-PC2
- 來源網路位址: 203.[redacted].17
- 來源連接埠: 11852



Time	Source	Event ID	Event Description
2019/9/12 下午 11:03:12	Microsoft-...	4624	帳戶成功登入。 主旨: 安全性識別碼: S-1-5-18 帳戶名稱: [redacted]N-PC2$
2019/9/12 下午 11:03:12	Microsoft-...	4624	帳戶成功登入。 主旨: 安全性識別碼: S-1-5-18 帳戶名稱: [redacted]N-PC2$

帳戶成功登入。

主旨:
- 安全性識別碼: S-1-5-18
- 帳戶名稱: [redacted]N-PC2$
- 帳戶網域: WORKGROUP
- 登入識別碼: 0x3e7

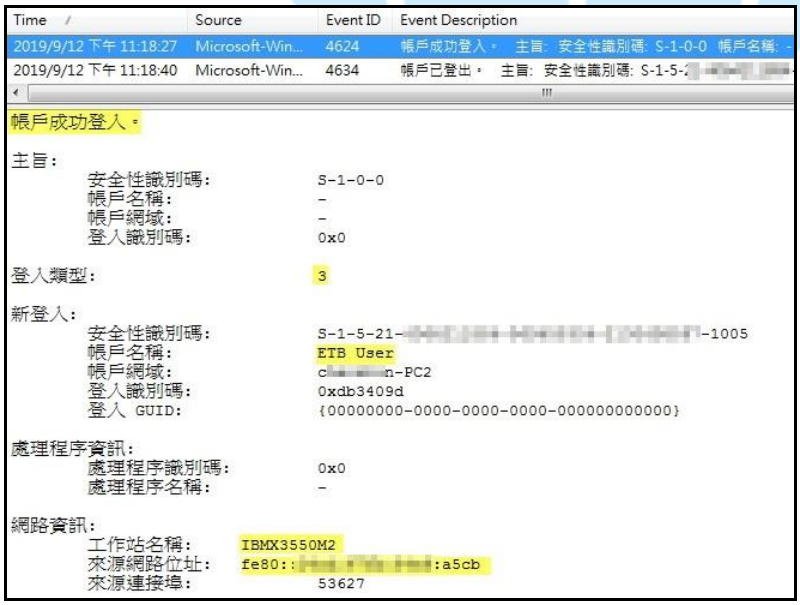
登入類型: 10

新登入:
- 安全性識別碼: S-1-5-21-[redacted]-1005
- 帳戶名稱: ETB User
- 帳戶網域: [redacted]n-PC2
- 登入識別碼: 0xd9dbd55
- 登入 GUID: {00000000-0000-0000-0000-000000000000}

處理程序資訊:
- 處理程序識別碼: 0x16dc
- 處理程序名稱: C:\Windows\System32\winlogon.exe

網路資訊:
- 工作站名稱: [redacted]N-PC2
- 來源網路位址: 203.[redacted].17
- 來源連接埠: 12076

在 2019/9/12 下午 11:18 有一個 IBMX3550M2 主機以帳戶 ETB User 網路連線登入 31 主機。



Time	Source	Event ID	Event Description
2019/9/12 下午 11:18:27	Microsoft-Win...	4624	帳戶成功登入。 主旨: 安全性識別碼: S-1-0-0 帳戶名稱:
2019/9/12 下午 11:18:40	Microsoft-Win...	4634	帳戶已登出。 主旨: 安全性識別碼: S-1-5-[redacted]

帳戶成功登入。

主旨:
- 安全性識別碼: S-1-0-0
- 帳戶名稱: -
- 帳戶網域: -
- 登入識別碼: 0x0

登入類型: 3

新登入:
- 安全性識別碼: S-1-5-21-[redacted]-1005
- 帳戶名稱: ETB User
- 帳戶網域: [redacted]n-PC2
- 登入識別碼: 0xdb3409d
- 登入 GUID: {00000000-0000-0000-0000-000000000000}

處理程序資訊:
- 處理程序識別碼: 0x0
- 處理程序名稱: -

網路資訊:
- 工作站名稱: IBMX3550M2
- 來源網路位址: fe80::[redacted]:a5cb
- 來源連接埠: 53627

4. 透過 lastactivityview 檢視 31 主機操作紀錄，發現在 9/12 下午 10:51 帳戶 ETB User 登入後，在下午 10:53 執行 Windows Installer，之後在 9/12 下午 11:03 再次登入主機執行 Windows Installer，在 9/17 上午 1:25 安裝 ScreenConnect Client，至 9/17 下午 4:12 帳戶 ETB User 登出。

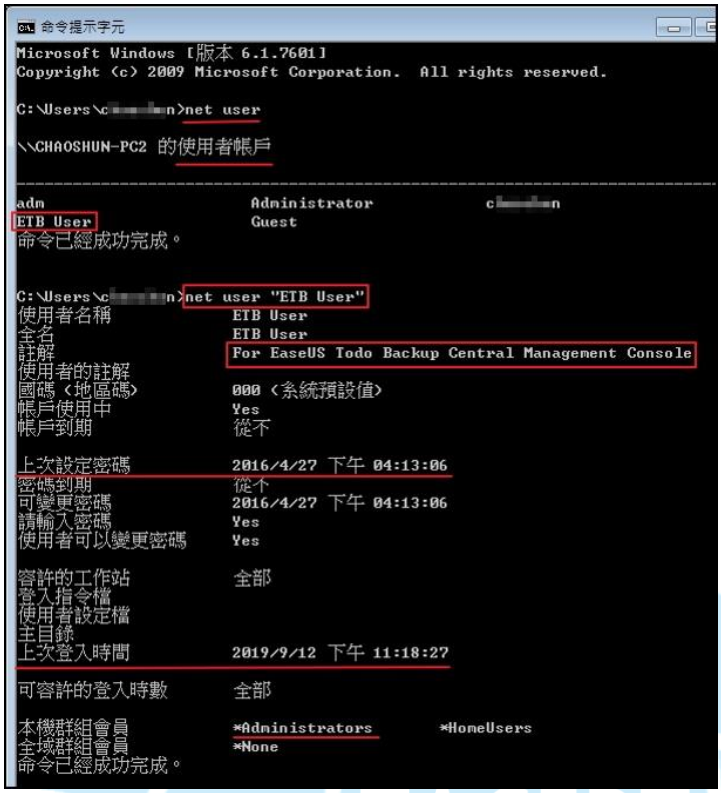
Action Time	Description	More Information
2019/9/17 下午 04:12:26	System Shutdown	
2019/9/17 下午 04:12:26	User Logoff	c[redacted]n-PC2\ETB User
2019/9/17 上午 02:21:55	Restore Point Created	
2019/9/17 上午 01:25:33	Windows Installer Ended	
2019/9/17 上午 01:25:32	Software Installation	ScreenConnect Client (efb8cf813b6eaefc)
2019/9/17 上午 01:25:29	Windows Installer Started	
2019/9/16 上午 01:00:00	User Logon	WORKGROUP\c[redacted]n
2019/9/13 上午 01:00:00	User Logon	WORKGROUP\c[redacted]n
2019/9/13 上午 12:00:16	Restore Point Created	
2019/9/12 下午 11:04:44	Windows Installer Ended	
2019/9/12 下午 11:04:37	Windows Installer Started	
2019/9/12 下午 11:04:02	Software Crash	Explorer.EXE, 6.1.7601.17567, 4d6727a7, mso.dll_unloaded, 0.0.0...
2019/9/12 下午 11:03:12	User Logon	WORKGROUP\ETB User
2019/9/12 下午 10:53:28	Windows Installer Ended	
2019/9/12 下午 10:53:21	Restore Point Created	
2019/9/12 下午 10:53:10	Windows Installer Started	
2019/9/12 下午 10:51:50	User Logon	WORKGROUP\ETB User
2019/9/12 上午 02:22:25	Restore Point Created	

5. 從 31 主機操作紀錄發現在 2016/4/27 下午 4:12 安裝過電腦備份還原軟體 EaseUS Todo Backup (第 6 版)，目前該軟體最新版為第 12.9 版，經查詢網路資訊，發現該軟體在第 5.8 版曾存在一個硬編碼(hardcoded)的管理密碼，該密碼可視為潛在的後門，為該軟體的一大漏洞，而本主機所安裝的第 6 版可能也存在此漏洞。

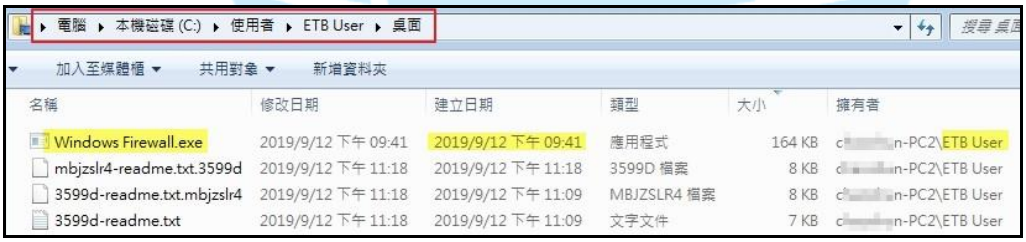
Action Time	Description	Full Path	More Information
2016/4/27 下午 04:12:56	Software Installation	C:\Program Files\EaseUS\Todo Backup\bin\Loader.exe	EaseUS Todo Backup Technician 6.0
2016/4/27 下午 04:10:47	Open file or folder	C:\Users\c[redacted]n\Downloads\EaseUS	
2016/4/27 下午 04:10:47	Open file or folder	C:\Users\c[redacted]n\Downloads\EaseUS\key.txt	
2016/4/27 下午 04:09:44	View Folder in Explorer	EaseUS	
2016/4/27 下午 04:08:55	User Logon		WORKGROUP\c[redacted]n

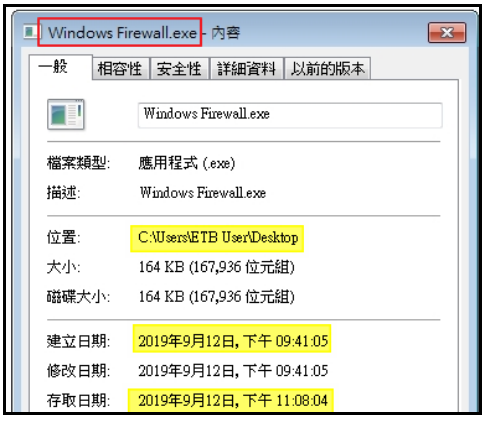
以 Net User 指令查看主機的使用者帳戶發現帳戶 ETB User 仍然使用中，檢視 ETB User 的帳戶資訊，發現該帳戶提供軟體 EaseUS Todo Backup 的 Central Management Console(中央管理控制台)使用。從 ETB User 帳戶資訊得知，該帳戶在 2016/4/27 下午 4:13 建立帳戶並設定預設密碼後，再無變更密碼，而且該帳戶具有系統管理者權限。此外，該帳戶上次登入時間 2019/9/12 下午

11:18 為本資安事件發生時間。

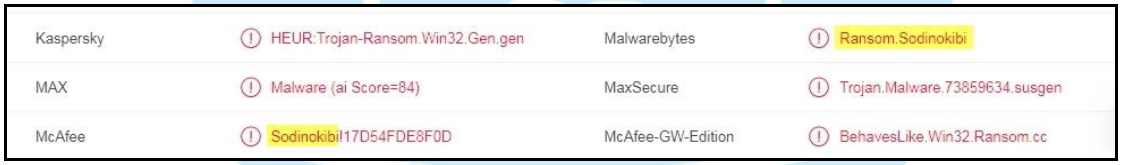


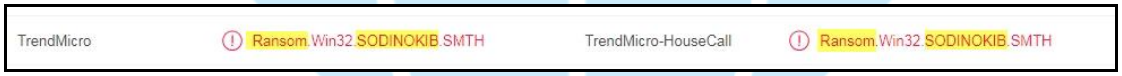
6. 在帳戶 ETB User 的桌面，發現一個在 2019/9/12 下午 9:41 建立的 Windows Firewall.exe 執行檔，其檔名易被視為防火牆之設定檔，而該檔案在 2019/9/12 下午 11:08 被執行過，其檔案建立時間下午 9:41 比 ETB User 資料夾建立時間同日下午 10:51 還要早，推測該檔案可能是從主機其他地方移入。





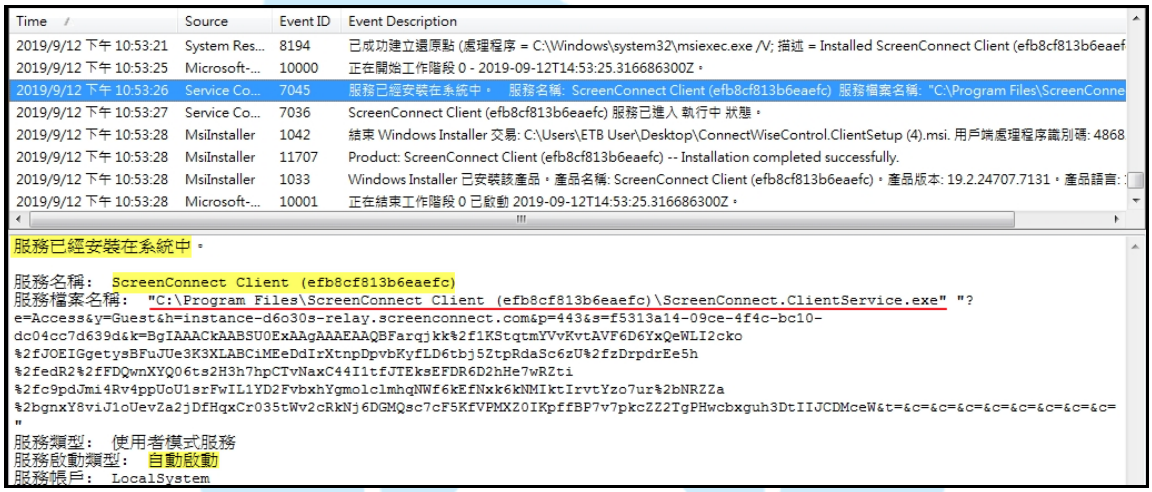
Windows Firewall.exe 經 Virustotal 檢測，其惡意比例為 45/67，有多家防毒軟體以 Ransom.Sodinokibi 命名它。



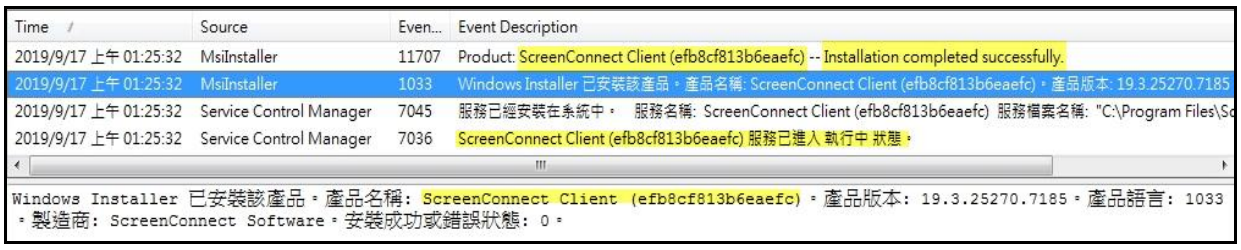


7. 從 31 主機的程式和功能內容，發現在 2019/9/17 曾安裝過 ScreenConnectClient(efb8cf813b6eaefc)。

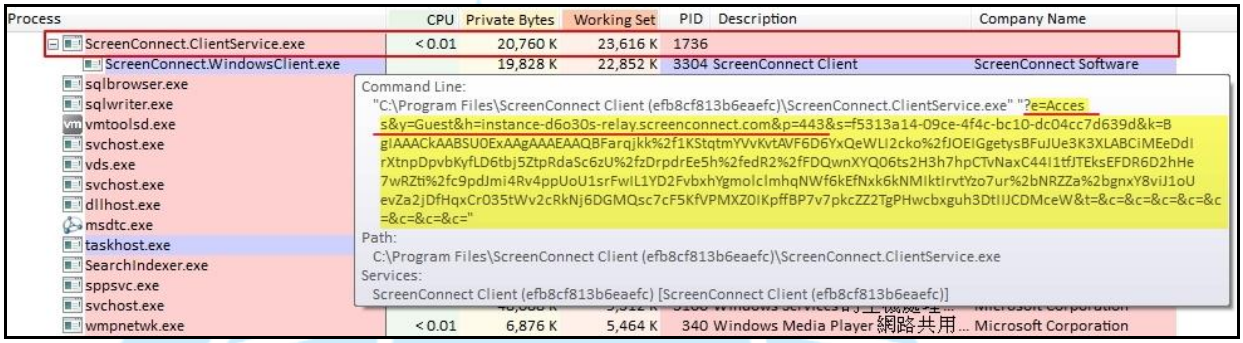
在主機的事件檢視紀錄內發現 2019/9/12 下午 10:53 曾安裝過 ScreenConnectClient(efb8cf813b6eaefc)，而且該程式會在開機後自動啟動。

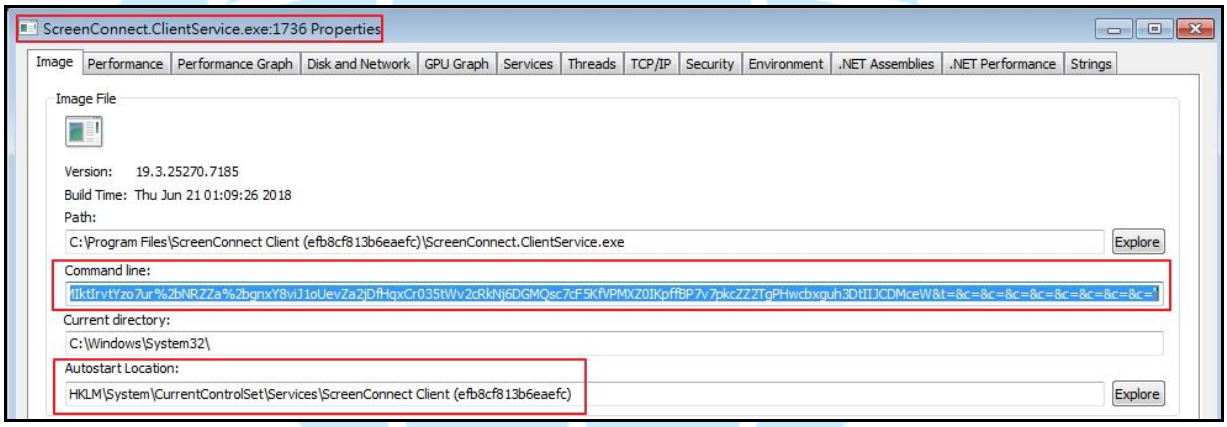


在 C:\Program Files 內 ScreenConnectClient(efb8cf813b6eaefc)資料夾的建立日期為 2019/9/17 上午 1:25，推測駭客將原先 2019/9/12 安裝的程式 ScreenConnectClient 移除重裝過。

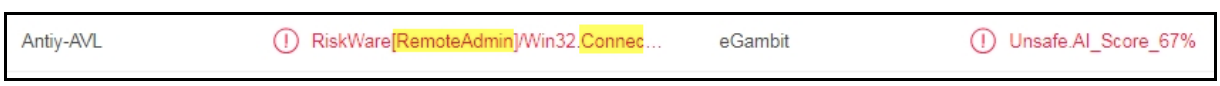


8. 在 C:\Program Files\ ScreenConnectClient(efb8cf813b6eaefc)資料夾內有兩個執行檔 ScreenConnect.ClientService.exe 與 ScreenConnect.WindowsClient.exe，而從主機背景程式運作情形得知，ScreenConnect.ClientService.exe 執行後會呼叫 ScreenConnect.WindowsClient.exe 來執行。檢視 ScreenConnect.ClientService.exe 屬性內容，發現該程式會在重新開機後自動執行。從執行的 Command line 內容得知，會以 Guest 身分存取網址 https://instance-d6o30s-replay.screenconnect.com，而其傳輸內容為加密內容。



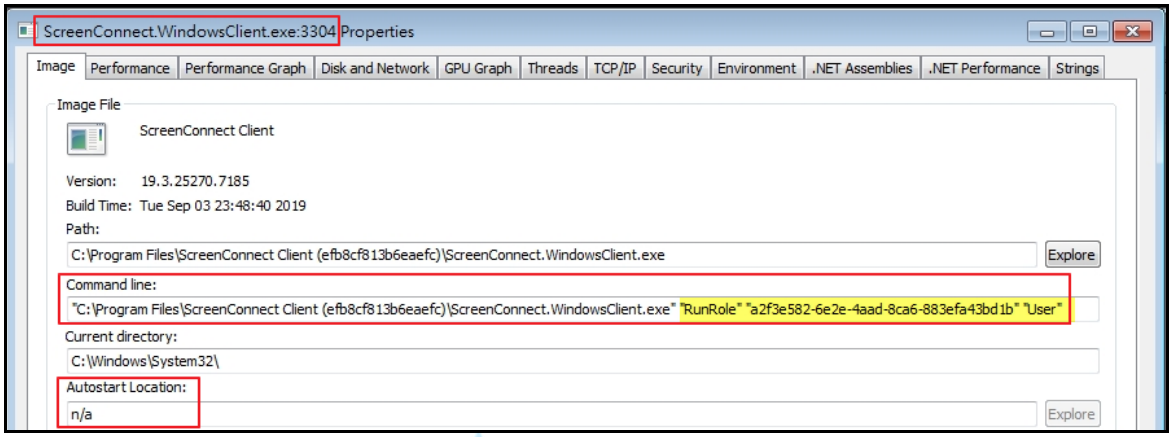


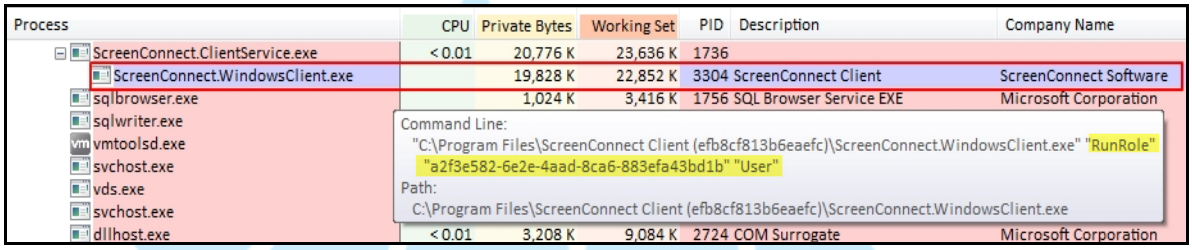
ScreenConnect.ClientService.exe 經 Virustotal 檢測其惡意比例為 2/69，表示大多數防毒軟體無法偵測出它的存在。



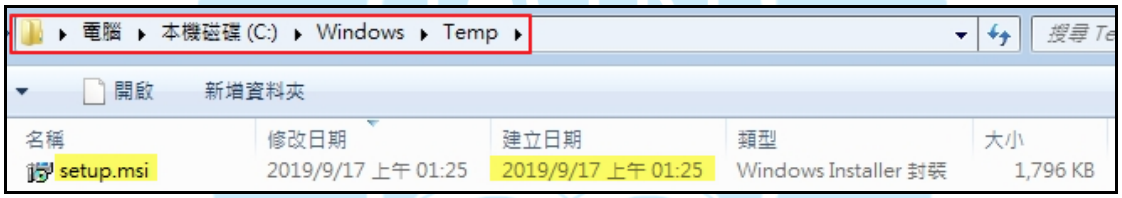
檢視 ScreenConnect.WindowsClient.exe 屬性內容，發現 Command line 內容為設定執行角色，而且該程式在主機開機後不會自動執行，但是會因為

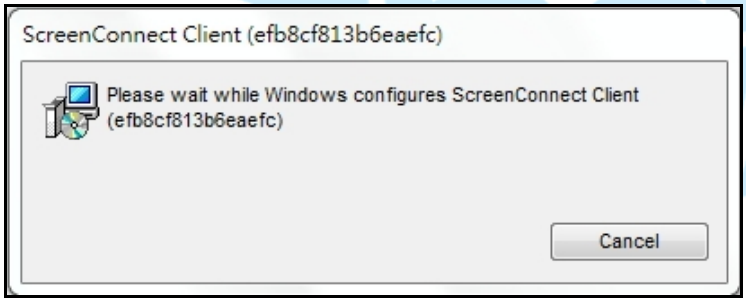
ScreenConnect.ClientService.exe 的呼叫而啟動。





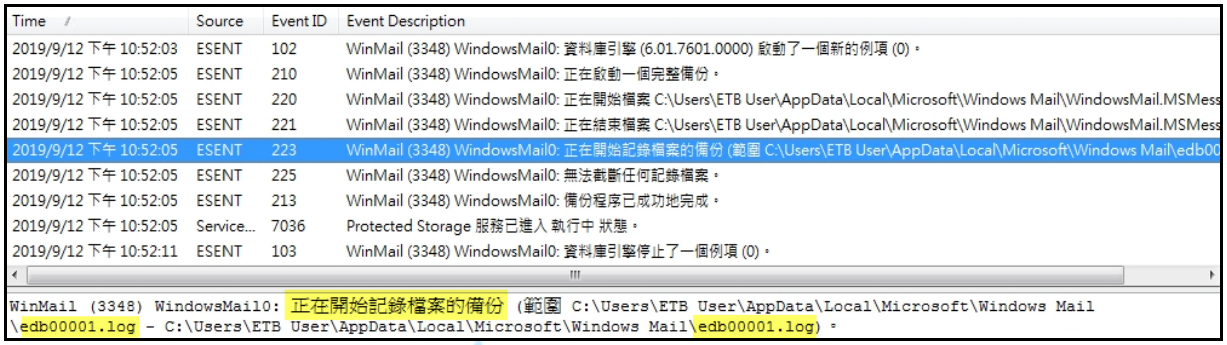
在 C:\windows\temp 內發現 setup.msi，執行 set.msi 後發現該程式會安裝 ScreenConnectClient(efb8cf813b6eaefc)。

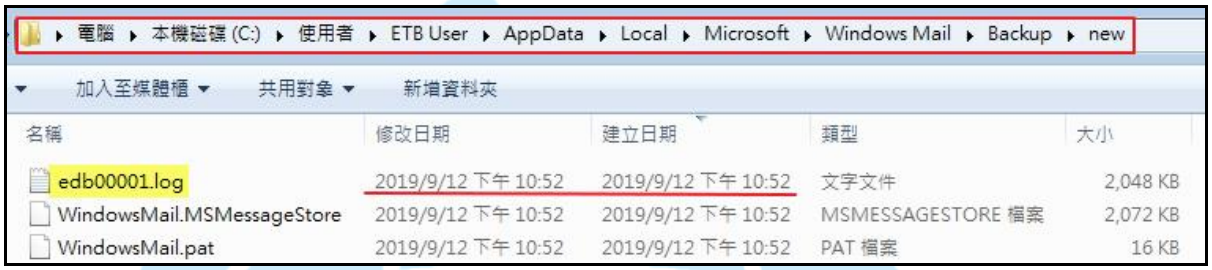




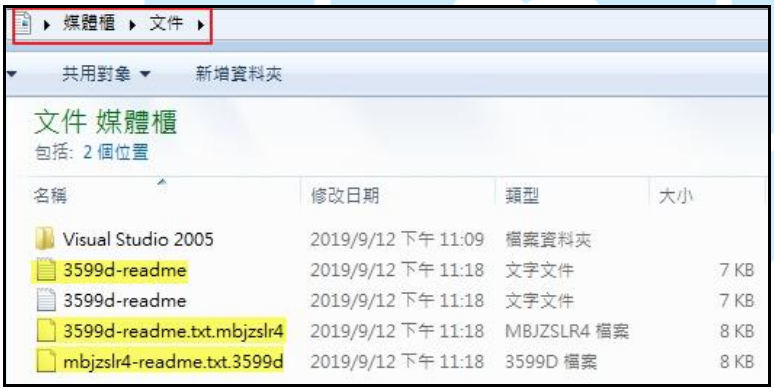
從事件檢視紀錄得知，2019/9/17 上午 1:25 所安裝的 ScreenConnectClient(efb8cf813b6eaefc)是執行 setup.msi 後所產生。

9. 從事件檢視紀錄發現駭客在 2019/9/12 下午 10:51 以帳戶 ETB User 登入主機後，在下午 10:52 執行 WindowsMail 的備份，並產生備份檔 edb00001.log。



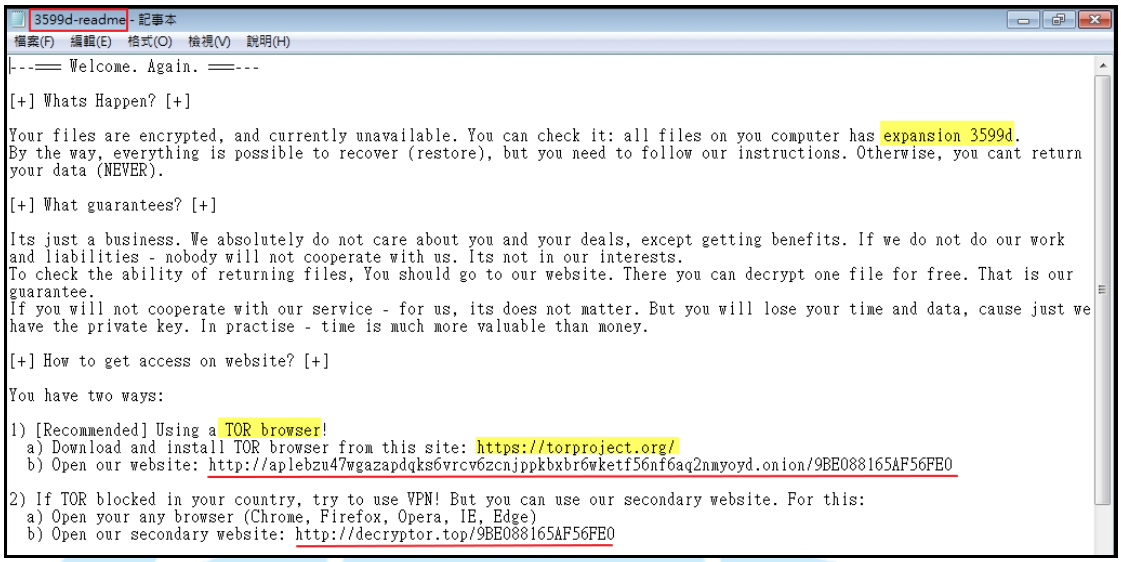


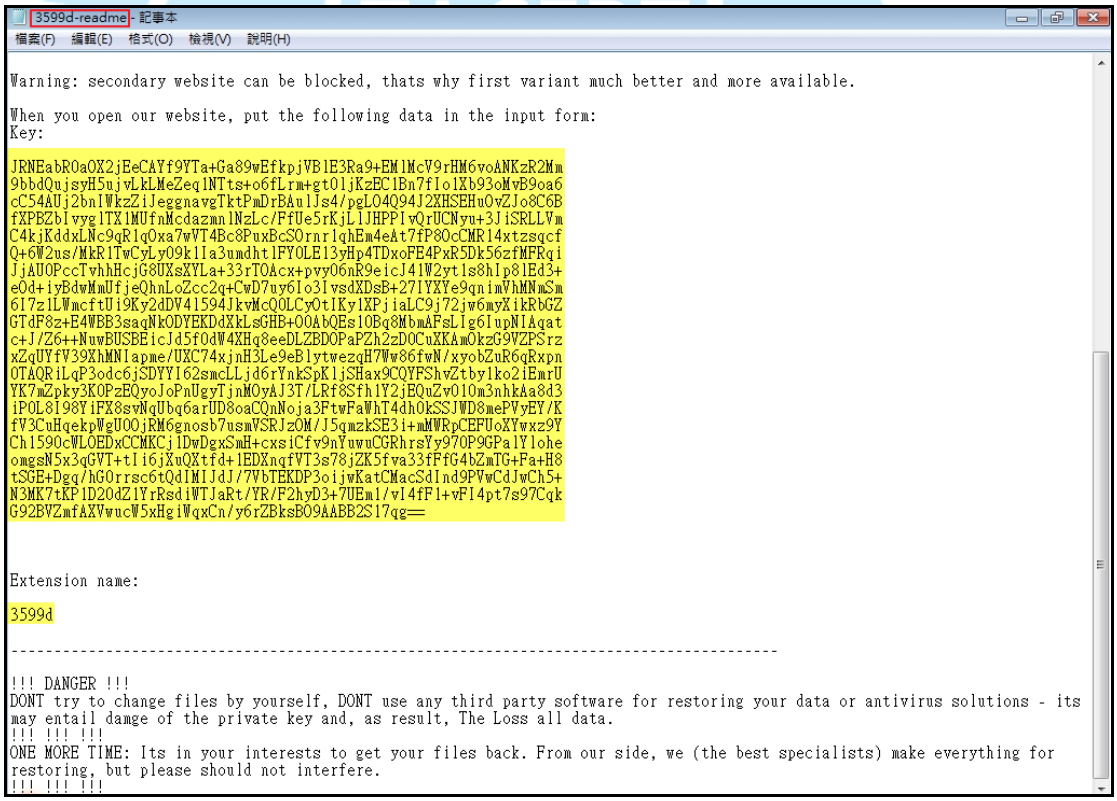
10. 查看 31 主機檔案被加密情形，發現除 C:\windows 外，檔案都被加密，加密過的資料夾會有 3599d-readme.txt，而有些有 3599d-readme.txt.mbjzslr4 與 mbjzslr4-readme.txt.3599d 兩個檔案。



所有被加密過的檔案會在檔名後延伸出 3599d 的副檔名，以「*.3599d」查詢所有主機內檔案，發現第一檔案被加密的時間點在 2019/9/12 下午 11:08，推測此為駭客執行勒索軟體的時間。

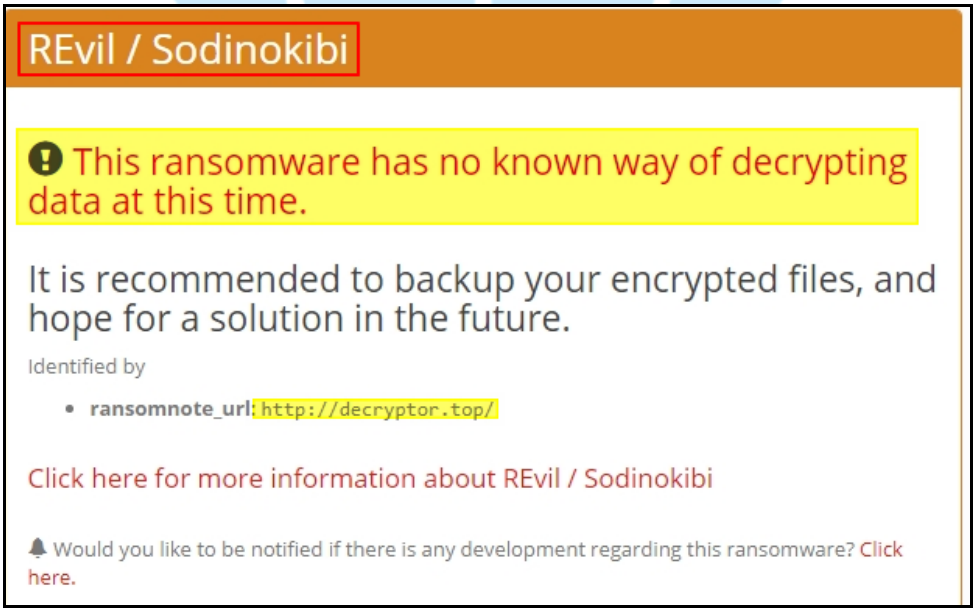
檢視 3599d-readme.txt 內容，發現此為勒索通知信，主要告訴受害者所有被加密的檔案都會延伸 3599d 的副檔名，也告訴受害者需透過洋蔥瀏覽器連結信中所提供的網址來取得付款資訊，而且在信件最後有提供一組加密的 key 給使用者連上網址後使用。



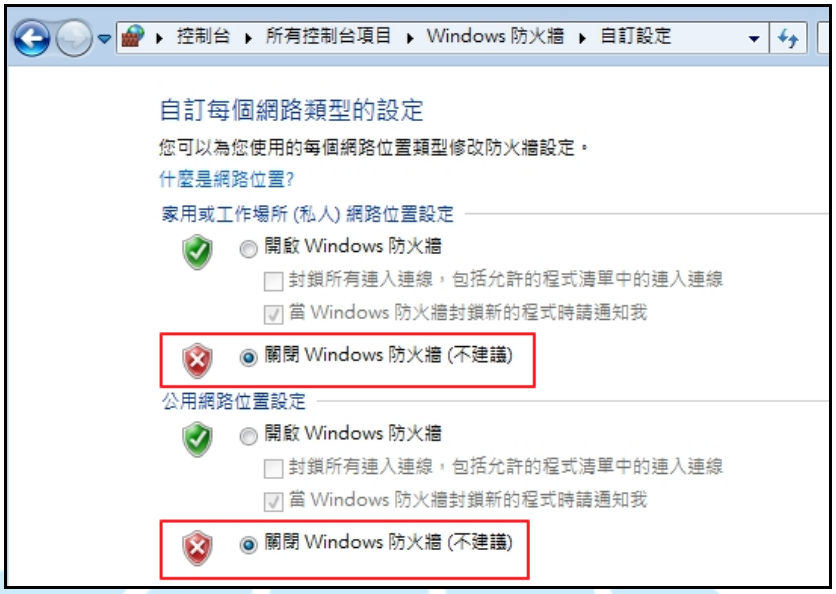


開啟 599d-readme.txt.mbjzslr4 與 mbjzslr4-readme.txt.3599d 兩個檔案，發現內容為亂碼，無法辨識。

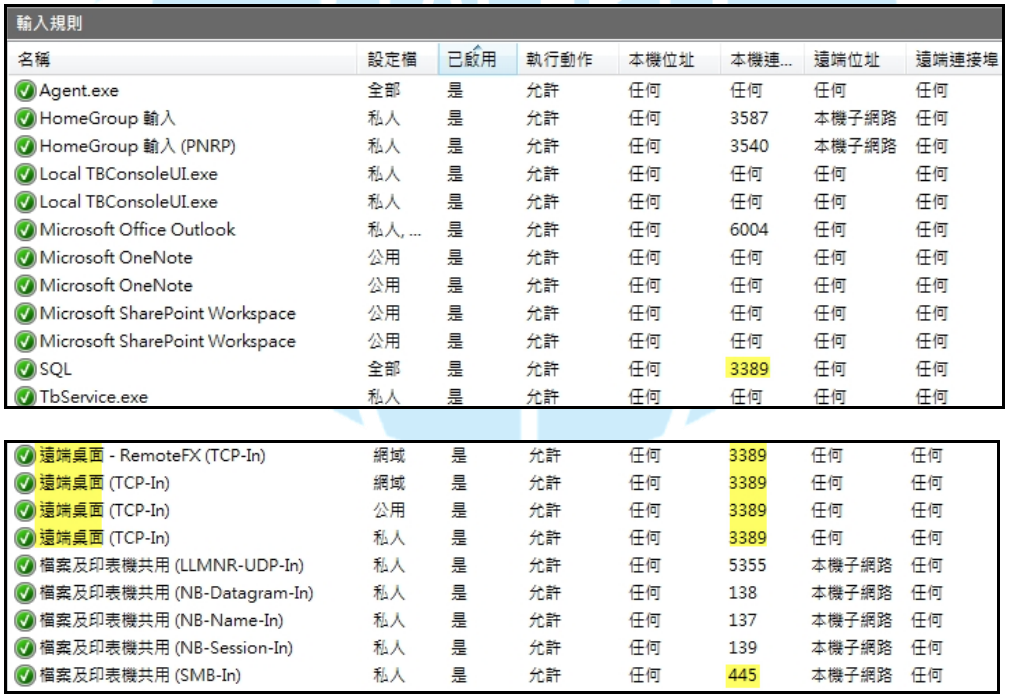
11. 將 3599d-readme.txt 與被加密的檔案上傳至 ID Ransomware 勒索病毒辨別網站(https://id-ransomware.malwarehunterteam.com)，經檢測判定為 Sodinokibi 勒索軟體，因此推測在 ETB User 桌面的 Windows Firewall.exe 為主機中毒來源，而駭客可能是以帳戶 ETB User 登入主機後，在主機上直接執行 Windows Firewall.exe，最後導致整個主機中毒。



12. 查看 31 主機的 Windows 防火牆設定，發現為關閉狀態，此種設定將降低主機的資安防護能力。



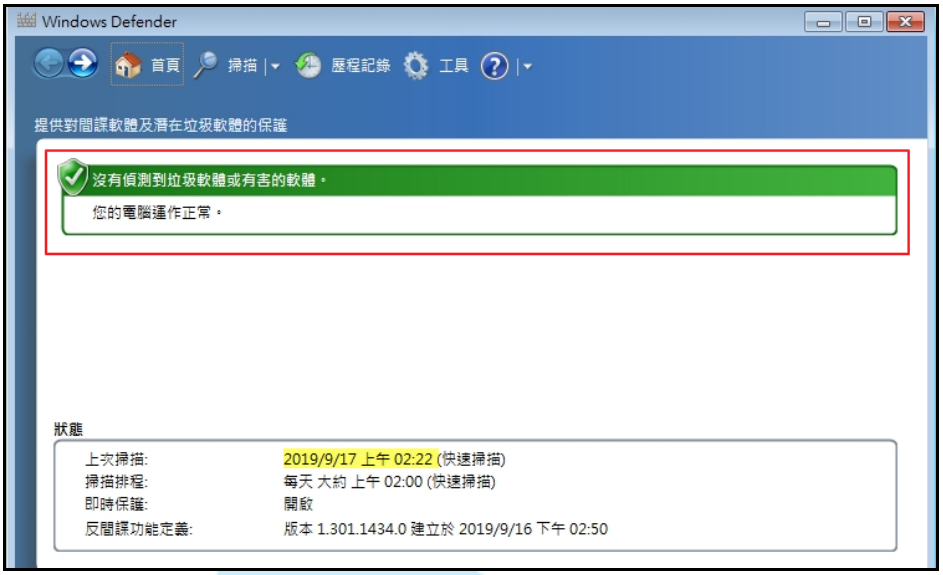
13. 檢視 31 主機的防火牆輸入規則設定，發現主機有開啟駭客常會攻擊的 3389port 與 445port。



輸入規則

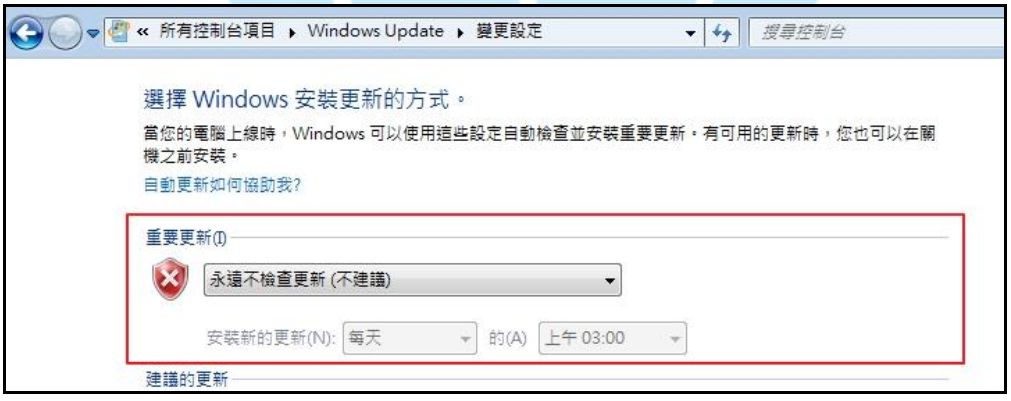
名稱	設定檔	已啟用	執行動作	本機位址	本機連...	遠端位址	遠端連接埠
Agent.exe	全部	是	允許	任何	任何	任何	任何
HomeGroup 輸入	私人	是	允許	任何	3587	本機子網路	任何
HomeGroup 輸入 (PNRP)	私人	是	允許	任何	3540	本機子網路	任何
Local TBConsoleUI.exe	私人	是	允許	任何	任何	任何	任何
Local TBConsoleUI.exe	私人	是	允許	任何	任何	任何	任何
Microsoft Office Outlook	私人, ...	是	允許	任何	6004	任何	任何
Microsoft OneNote	公用	是	允許	任何	任何	任何	任何
Microsoft OneNote	公用	是	允許	任何	任何	任何	任何
Microsoft SharePoint Workspace	公用	是	允許	任何	任何	任何	任何
Microsoft SharePoint Workspace	公用	是	允許	任何	任何	任何	任何
SQL	全部	是	允許	任何	3389	任何	任何
TbService.exe	私人	是	允許	任何	任何	任何	任何
遠端桌面 - RemoteFX (TCP-In)	網域	是	允許	任何	3389	任何	任何
遠端桌面 (TCP-In)	網域	是	允許	任何	3389	任何	任何
遠端桌面 (TCP-In)	公用	是	允許	任何	3389	任何	任何
遠端桌面 (TCP-In)	私人	是	允許	任何	3389	任何	任何
檔案及印表機共用 (LLMNR-UDP-In)	私人	是	允許	任何	5355	本機子網路	任何
檔案及印表機共用 (NB-Datagram-In)	私人	是	允許	任何	138	本機子網路	任何
檔案及印表機共用 (NB-Name-In)	私人	是	允許	任何	137	本機子網路	任何
檔案及印表機共用 (NB-Session-In)	私人	是	允許	任何	139	本機子網路	任何
檔案及印表機共用 (SMB-In)	私人	是	允許	任何	445	本機子網路	任何

14. 檢視 31 主機的防毒軟體 Windows Defender 內容，發現最近一次掃描為 2019/9/17 上午 2:22，但是卻無法發現惡意軟體 windows firewall.exe 存在於主機內。

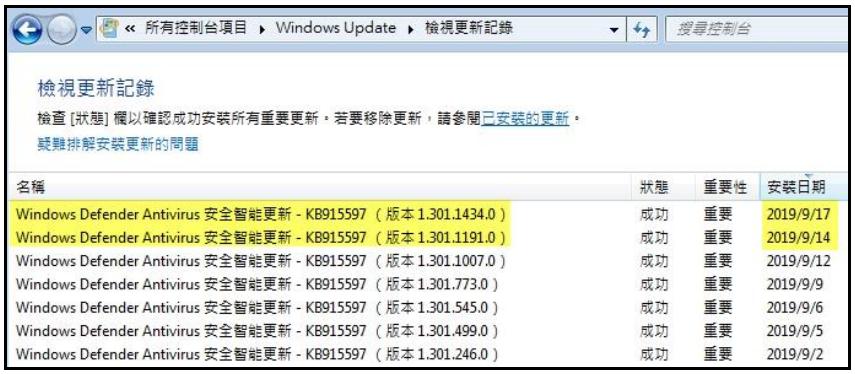


查看主機 Windows update 更新系統狀態，發現該主機從未進行過系統更新。

從 Windows update 設定內容，發現該主機設定為「永遠不檢查更新」，此將導致系統漏洞無法修補，降低駭客駭入主機的困難性。

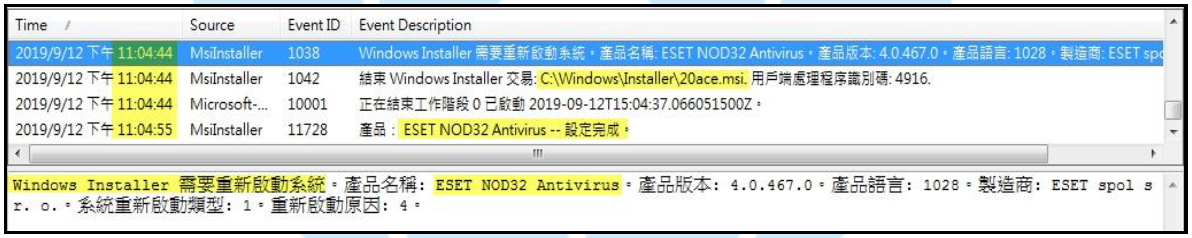


檢視更新記錄得知，該主機有定期更新 Windows Defender，但是無法防禦 Sodinokibi 勒索軟體的攻擊。



15.從事件檢視紀錄發現 2019/9/12 下午 11:04 駭客曾經利用 C:\Windows\Installer 資料夾內的 20ace.msi，來安裝 ESET NOD32 Antivirus 防毒軟體，但檢測 31 主機時，在 C:\Windows 內已找不到 Installer 資料夾與 20ace.msi。

Time	Source	Event ID	Event Description
2019/9/12 下午 11:04:27	Service Control Manager	7036	Windows Installer 服務已進入 執行中 狀態。
2019/9/12 下午 11:04:37	MsiInstaller	1040	開始 Windows Installer 交易: C:\Windows\Installer\20ace.msi。用戶端處理程序識別碼: 4916。
2019/9/12 下午 11:04:37	Microsoft-Windows-RestartManager	10000	正在開始工作階段 0 - 2019-09-12T15:04:37.066051500Z。
2019/9/12 下午 11:04:37	Microsoft-Windows-RestartManager	10005	機器必須重新啟動。
2019/9/12 下午 11:04:42	Service Control Manager	7036	ESET Service 服務已進入 停止 狀態。
2019/9/12 下午 11:04:44	MsiInstaller	1038	Windows Installer 需要重新啟動系統。產品名稱: ESET NOD32 Antivirus。產品版本: 4.0.467.0。產品語言: 1028。製造商: ESET
2019/9/12 下午 11:04:44	MsiInstaller	1042	結束 Windows Installer 交易: C:\Windows\Installer\20ace.msi. 用戶端處理程序識別碼: 4916.
2019/9/12 下午 11:04:44	Microsoft-Windows-RestartManager	10001	正在結束工作階段 0 已啟動 2019-09-12T15:04:37.066051500Z。
2019/9/12 下午 11:04:55	MsiInstaller	11728	產品： ESET NOD32 Antivirus -- 設定完成。
2019/9/12 下午 11:04:55	MsiInstaller	1035	Windows Installer 已重新設定該產品。產品名稱: ESET NOD32 Antivirus。產品版本: 4.0.467.0。產品語言: 1028。製造商: ESET
2019/9/12 下午 11:04:55	MsiInstaller	1038	Windows Installer 需要重新啟動系統。產品名稱: ESET NOD32 Antivirus。產品版本: 4.0.467.0。產品語言: 1028。製造商: ESET
2019/9/12 下午 11:04:55	MsiInstaller	1029	產品: ESET NOD32 Antivirus。必須重新啟動，產品的安裝或更新需要重新啟動，所有變更才會生效。重新啟動已順延至稍後。
2019/9/12 下午 11:06:02	Service Control Manager	7036	Windows Error Reporting Service 服務已進入 停止 狀態。



Time	Source	Event ID	Event Description
2019/9/12 下午 11:04:44	MsiInstaller	1038	Windows Installer 需要重新啟動系統。產品名稱: ESET NOD32 Antivirus。產品版本: 4.0.467.0。產品語言: 1028。製造商: ESET spo
2019/9/12 下午 11:04:44	MsiInstaller	1042	結束 Windows Installer 交易: C:\Windows\Installer\20ace.msi. 用戶端處理程序識別碼: 4916.
2019/9/12 下午 11:04:44	Microsoft-...	10001	正在結束工作階段 0 已啟動 2019-09-12T15:04:37.066051500Z。
2019/9/12 下午 11:04:55	MsiInstaller	11728	產品： ESET NOD32 Antivirus -- 設定完成。

Windows Installer 需要重新啟動系統。產品名稱: ESET NOD32 Antivirus。產品版本: 4.0.467.0。產品語言: 1028。製造商: ESET spol s r. o.。系統重新啟動類型: 1。重新啟動原因: 4。

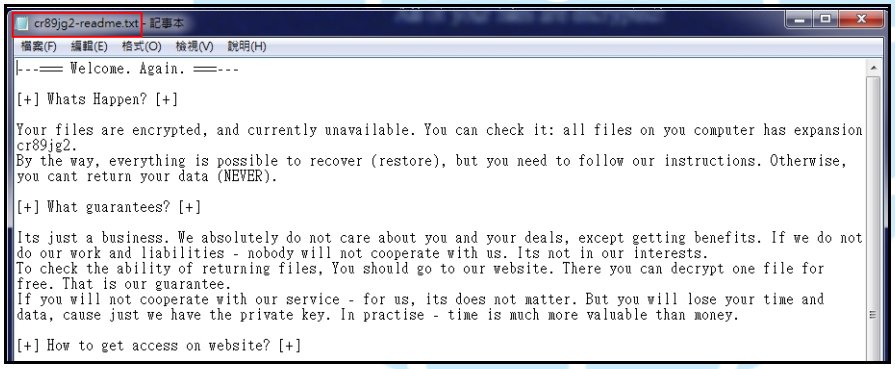
16.由事件檢視紀錄可得知，在 2019/9/12 下午 11:08 駭客執行 8 次 PowerShell，此時間為 Sodinokibi 勒索軟體加密主機檔案的時間，推測這些 PowerShell 的執行或許與 Sodinokibi 勒索軟體有關。

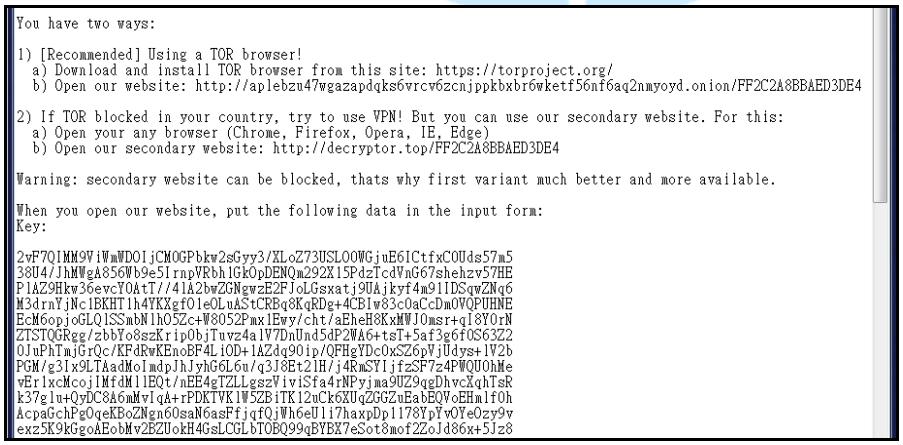
Time	Source	Event ID	Event Description
2019/9/12 下午 11:08:40	Service Control ...	7036	Microsoft Software Shadow Copy Provider 服務已進入 執行中 狀態。
2019/9/12 下午 11:08:40	PowerShell	600	"WSMan" 提供者為 Started。 詳細資料: ProviderName=WSMan NewProviderState=Started SequenceNumber=1 H
2019/9/12 下午 11:08:40	PowerShell	600	"Alias" 提供者為 Started。 詳細資料: ProviderName=Alias NewProviderState=Started SequenceNumber=2 HostNa
2019/9/12 下午 11:08:40	PowerShell	600	"Environment" 提供者為 Started。 詳細資料: ProviderName=Environment NewProviderState=Started SequenceNum
2019/9/12 下午 11:08:40	PowerShell	600	"FileSystem" 提供者為 Started。 詳細資料: ProviderName=FileSystem NewProviderState=Started SequenceNumber=
2019/9/12 下午 11:08:40	PowerShell	600	"Function" 提供者為 Started。 詳細資料: ProviderName=Function NewProviderState=Started SequenceNumber=5
2019/9/12 下午 11:08:40	PowerShell	600	"Registry" 提供者為 Started。 詳細資料: ProviderName=Registry NewProviderState=Started SequenceNumber=6 H
2019/9/12 下午 11:08:40	PowerShell	600	"Variable" 提供者為 Started。 詳細資料: ProviderName=Variable NewProviderState=Started SequenceNumber=7 H
2019/9/12 下午 11:08:40	PowerShell	600	"Certificate" 提供者為 Started。 詳細資料: ProviderName=Certificate NewProviderState=Started SequenceNumber=
2019/9/12 下午 11:08:40	PowerShell	400	引擎狀態已從 None 變更為 Available。 詳細資料: NewEngineState=Available PreviousEngineState=None SequenceN
2019/9/12 下午 11:08:53	PowerShell	403	引擎狀態已從 Available 變更為 Stopped。 詳細資料: NewEngineState=Stopped PreviousEngineState=Available Sequ

17.實際執行程式 windows firewall.exe，來查看其執行後會產生何種攻擊行為，而執行結果如下所示。

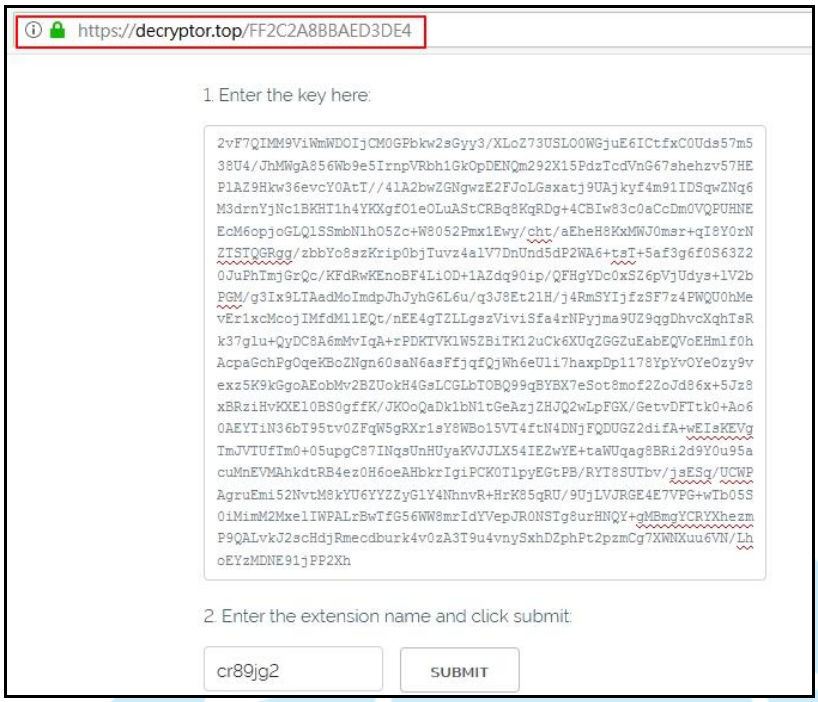
(1)在程式 windows firewall.exe 執行後，主機桌面會變成藍色，並且有提醒語「All of your files are encrypted!Find cr89jg2-readme.txt and follow instuctions」呈現於桌面，告訴受害者所有檔案已被加密，要去找到 cr89jg2-readme.txt，並且遵從檔案內指令。一段小段時間後，藍色桌面與提醒語在檔案加密完成後便會消失不見。

(2)查看 cr89jg2-readme.txt 內容，發現與 31 主機的勒索通知信 3599d-readme.txt 相同。

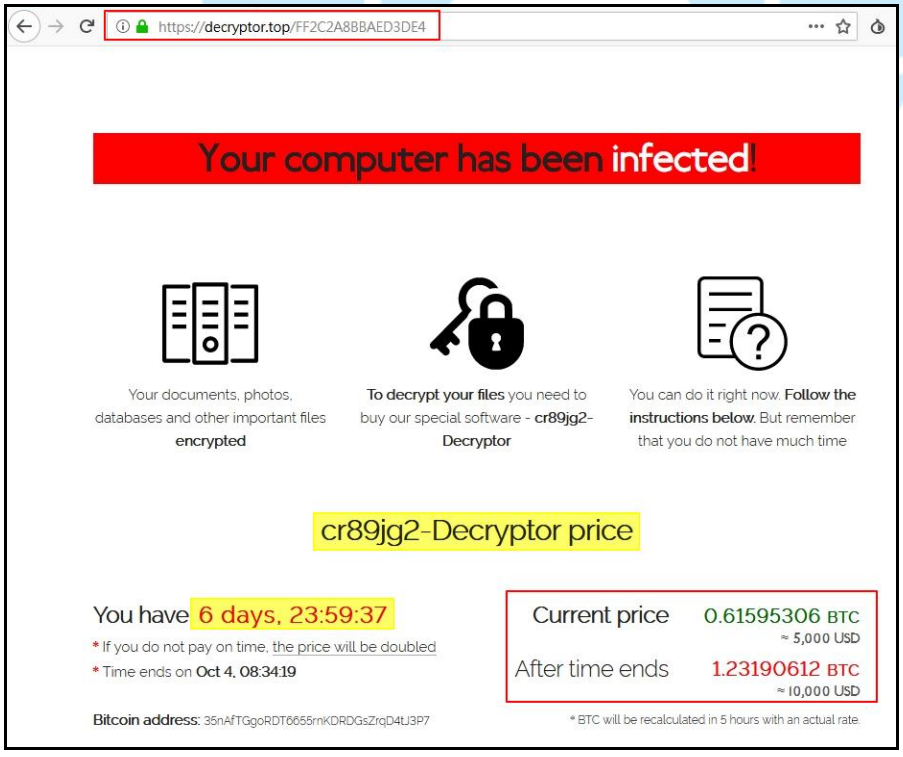




利用洋蔥瀏覽器開啟駭客所提供的連結網頁，將勒索通知信內的一段亂碼 Key 貼上，並且輸入延伸副檔名後送出，即可看到駭客所要求的付款資訊。



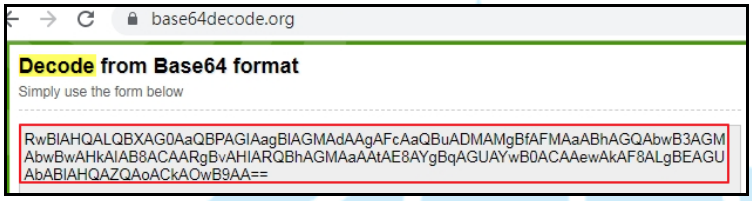
在付款資訊的網頁中，駭客告訴受害者解密器的價錢，而且 7 天後才付款則會價錢加倍，也告訴受害者如何付款，以及提供受害者上傳一個圖檔來測試解密器是否有效的機會。



(3) 在程式 windows firewall.exe 執行後會呼叫 powershell.exe 來執行一段加密過的亂碼命令，此呼叫 powershell.exe 的行為與 31 主機事件檢視紀錄中出現的 8 次 powershell 紀錄相似，推測這 8 次 powershell 紀錄應該是執行 windows firewall.exe 所造成。

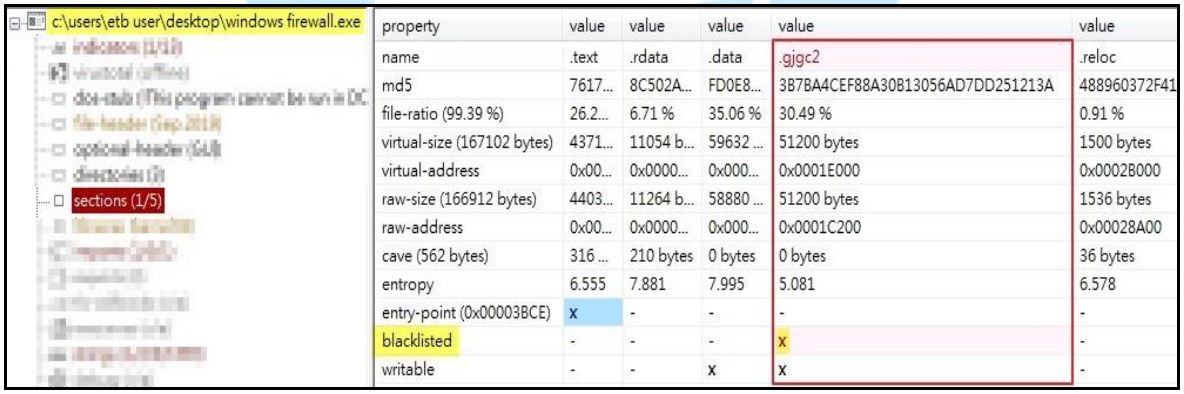
Process	Image Path	Command
Windows Firewall.exe (1560)	C:\Users\Mark\Downloads\Windows Firewall.exe	"C:\Users\Mark\Downloads\Windows Firewall.exe"
Windows Firewall.exe (664)	C:\Users\Mark\Downloads\Windows Firewall.exe	"C:\Users\Mark\Downloads\Windows Firewall.exe"
powershell.exe (2028)	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell -e RwBlAHQALQBXAG0AaQBPAGIAagBlAGMAdAAgAFcAaQ

將亂碼命令解碼後發現為刪除影子副本的命令。

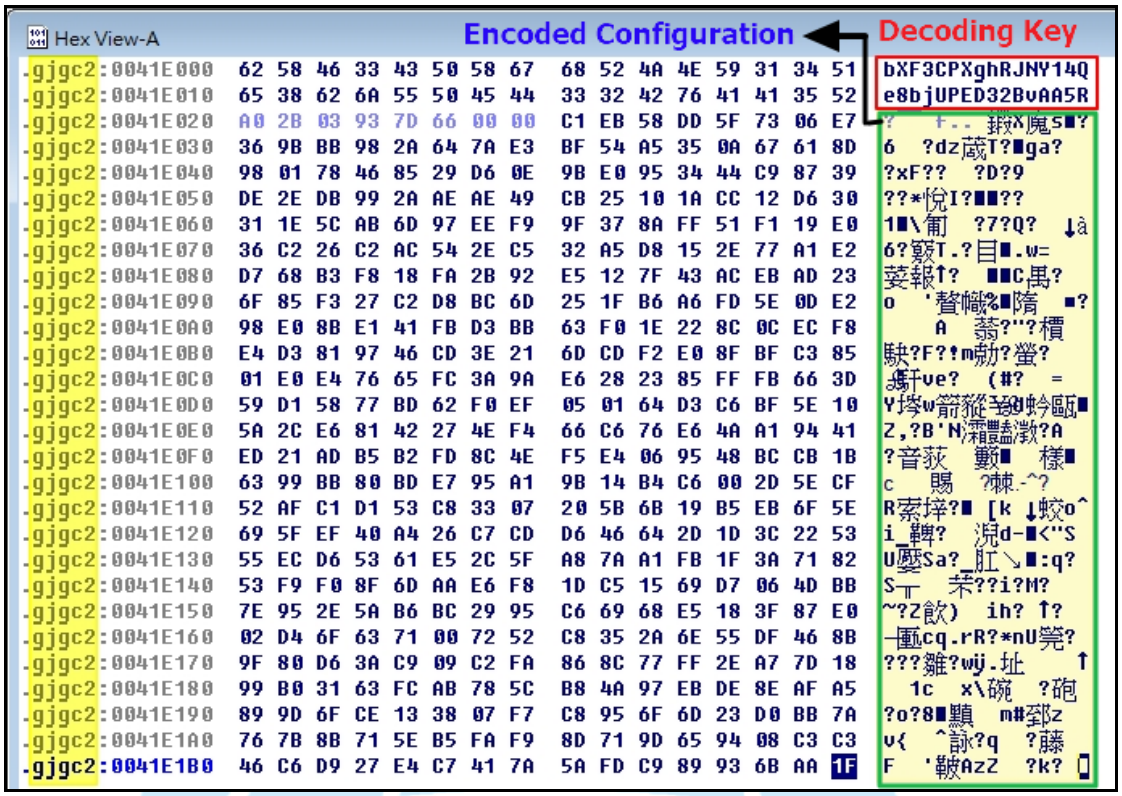



```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

(4)對 Windows firewall.exe 進行程式碼檢測，發現在 section 內容的配置資源.gjgc2 是被列入黑名單，其中此資源的前 32 個字節是用於解碼配置的密鑰「bXF3CPXghRJNY14Qe8bjUPED32BvAA5R」，而其餘字節是編碼配置。

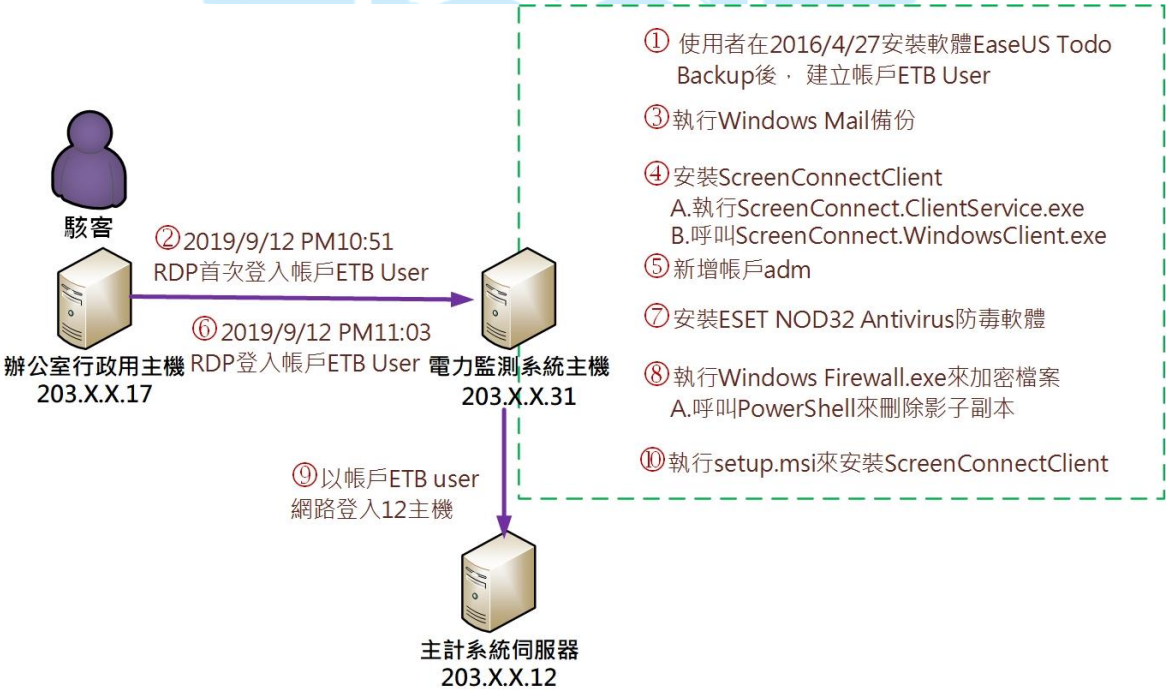


property	value	value	value	value	value
name	.text	.rdata	.data	.gjgc2	.reloc
md5	7617...	8C502A...	FD0E8...	3B7BA4CEF88A30B13056AD7DD251213A	488960372F41
file-ratio (99.39 %)	26.2...	6.71 %	35.06 %	30.49 %	0.91 %
virtual-size (167102 bytes)	4371...	11054 b...	59632 ...	51200 bytes	1500 bytes
virtual-address	0x00...	0x0000...	0x000...	0x0001E000	0x0002B000
raw-size (166912 bytes)	4403...	11264 b...	58880 ...	51200 bytes	1536 bytes
raw-address	0x00...	0x0000...	0x000...	0x0001C200	0x00028A00
cave (562 bytes)	316 ...	210 bytes	0 bytes	0 bytes	36 bytes
entropy	6.555	7.881	7.995	5.081	6.578
entry-point (0x00003BCE)	x	-	-	-	-
blacklisted	-	-	-	x	-
writable	-	-	x	x	-



三、事件攻擊行為示意圖

本事件雖牽涉多台主機，但由於取證資訊有限，將以鑑識電力監測系統主機(31 主機)為主，來呈現駭客的攻擊行為。



1. 使用者在 2016/4/27 下午 4:12 安裝電腦備份還原軟體 EaseUS Todo Backup 後，建立帳戶 ETB User。
2. 駭客在 2019/9/12 下午 10:51 首次遠端桌面連線登入帳戶 ETB User。
3. 在 2019/9/12 下午 10:52 執行 Windows Mail 備份(產生 edb00001.log)。
4. 在 2019/9/12 下午 10:53 安裝 ScreenConnectClient(efb8cf813b6eaefc)。
   A. 執行 ScreenConnect.ClientService.exe
   B. 呼叫 ScreenConnect.WindowsClient.exe
5. 在 2019/9/12 下午 10:58 建立使用者帳戶 adm。
6. 在 2019/9/12 下午 11:03 再次遠端桌面連線登入帳戶 ETB User。
7. 在 2019/9/12 下午 11:04 執行 20ace.msi 來安裝 ESET NOD32 Antivirus 防毒軟體。
8. 在 2019/9/12 下午 11:08 執行 Windows Firewall.exe 來加密主機內檔案。
   A. Windows Firewall.exe 呼叫 PowerShell 來刪除影子副本。
9. 2019/9/12 PM 11:11 以帳戶 ETB user 網路登入 12 主機。
10. 在 2019/9/17 上午 1:25 執行 setup.msi 來再次安裝 ScreenConnectClient (efb8cf813b6eaefc)。

四、總結與建議

1. Sodinokibi（也稱為 REvil）勒索軟體於 2019 年 4 月 17 日首次被發現。它是由有經濟動機的 GOLD SOUTHFIELD 威脅組織使用的，該組織通過漏

洞利用工具包、掃描漏洞技術、RDP 伺服器和有後門軟體安裝程式來散播勒索軟體。它可以利用 CVE-2018-8453 漏洞提升特權，成功利用此漏洞的攻擊者可以在內核模式下運行任意代碼。 然後，攻擊者可能會安裝程式、查看、更改或刪除資料；或者建立具有系統管理者權限的新帳戶。從本案的攻擊行為，可以明確地看到駭客充分運用勒索軟體 Sodinokibi 的散播手法來進行攻擊。

2. 從本資安事件的發生，可歸納出下列幾點資安防護漏洞提供參考。
   (1) 受害主機的系統版本老舊，Windows update 未開啟檢查更新設定。
   (2) 受害主機的防火牆未開啟。
   (3) 受害主機開啟許多容易受駭客攻擊的 port，如 3389 port 與 445 port。
   (4) 受害主機所安裝的防毒軟體無法識別 Windows firewall.exe 為 Sodinokibi 勒索軟體。
   (5) 在 2016/4/27 建立的帳戶 ETB User 可能存在硬編碼的管理密碼漏洞。
   (6) 從與管理者訪談得知，廠商使用簡易的相同密碼登入各主機來進行維護作業，降低駭客入侵的困難度，也容易遭受密碼填充攻擊。
   (7) 駭客在駭入含有 EaseUS Todo Backup 軟體所產生的帳戶 ETB User 之主機後，向同一區域網路內含有帳戶 ETB User 的各主機進行攻擊。
   (8) 本事件中各主機感染 Sodinokibi 勒索軟體的方式，推測是駭客駭入各主機後手動執行 Sodinokibi 的惡意程式造成感染。
3. 針對本資安事件建議下列幾點資安防護措施，提供大家參考。
   (1) 定期進行系統更新。
   (2) 開啟主機上的防火牆設定。
   (3) 關閉主機上非必要開啟的 port。
   (4) 更換功能更強大的防毒軟體，並定期更新病毒碼。
   (5) 定期備份主機資料。

(6) 定期檢視主機狀態，如連線紀錄、使用者帳戶資訊。

(7) 強化使用者密碼設定的複雜度。

(8) 管理者在管理區域網路內各主機時，勿使用同一組帳戶與密碼來登入各主機。

(9) 避免使用網路芳鄰進行檔案分享，建議關閉非必要使用的網路磁碟機。

(10) 更新軟體 EaseUS Todo Backup 之版本，來修補硬編碼的管理密碼漏洞。

五、相關資料

1. REvil/Sodinokibi Ransomware

https://www.secureworks.com/research/revil-sodinokibi-ransomware