勒索病毒 GlobeImposter 2.0 攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 07 月

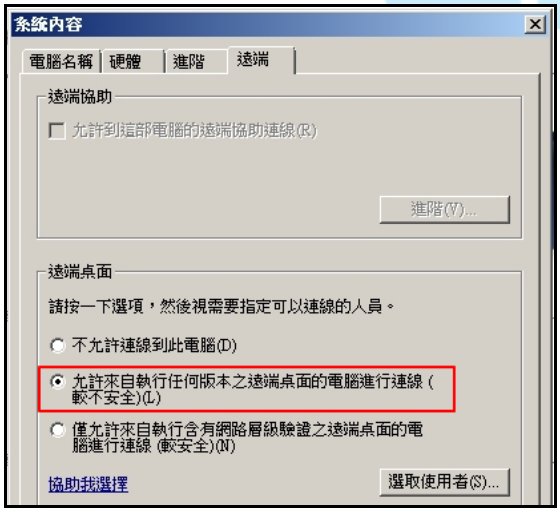
一、事件簡介

1. 2020 年 3 月底某學校有多台主機感染勒索病毒，為了瞭解該病毒對於受害主機的感染途徑與所造成的危害程度，對該校所提供的一台受害虛擬主機進行鑑識作業。

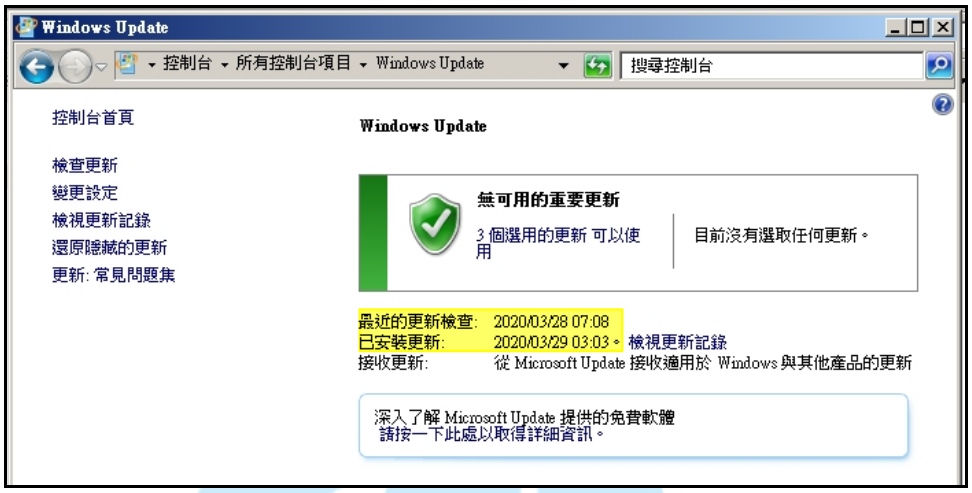
二、事件檢測

1. 首先，從系統資訊確認主機系統為 Windows Server 2008R2 Standard，但處理器與記憶體資訊無法得知。

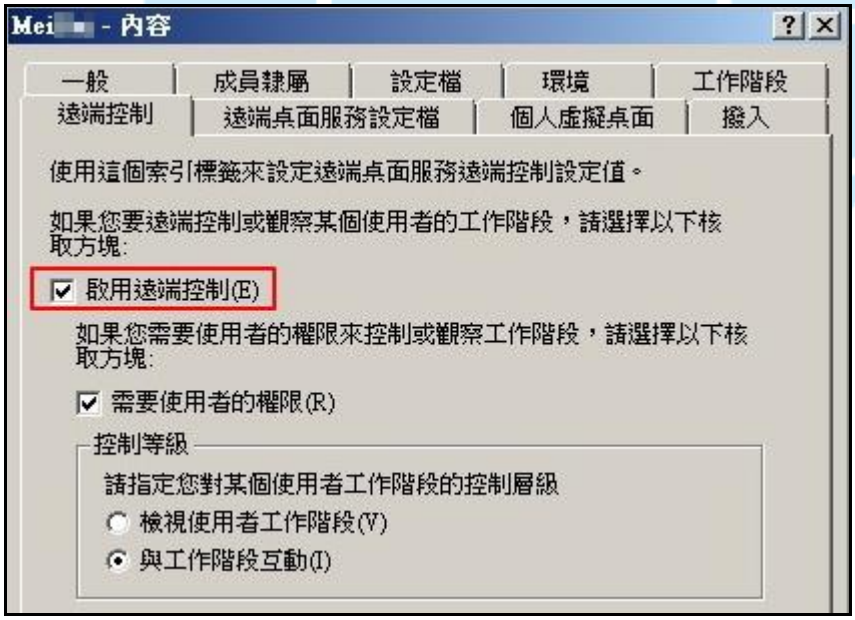
在系統內容中發現該主機設定允許來自執行任何版本之遠端桌面的電腦進行連線。



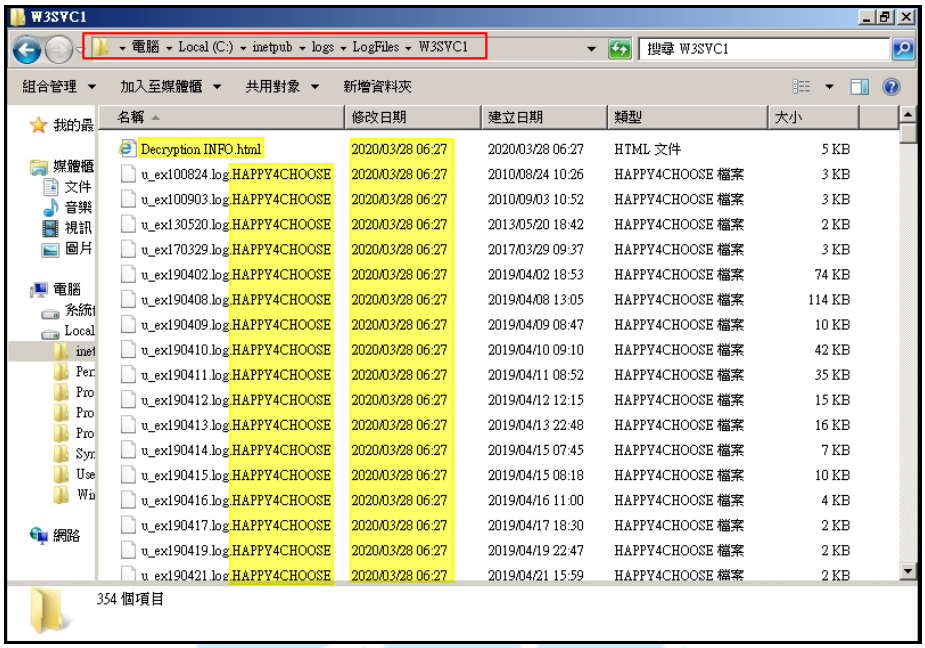
2. 該主機有開啟防火牆設定，並且各使用者帳戶皆有設定密碼保護，但該主機管理者有使用同一組帳號與密碼管理多台主機的現象。



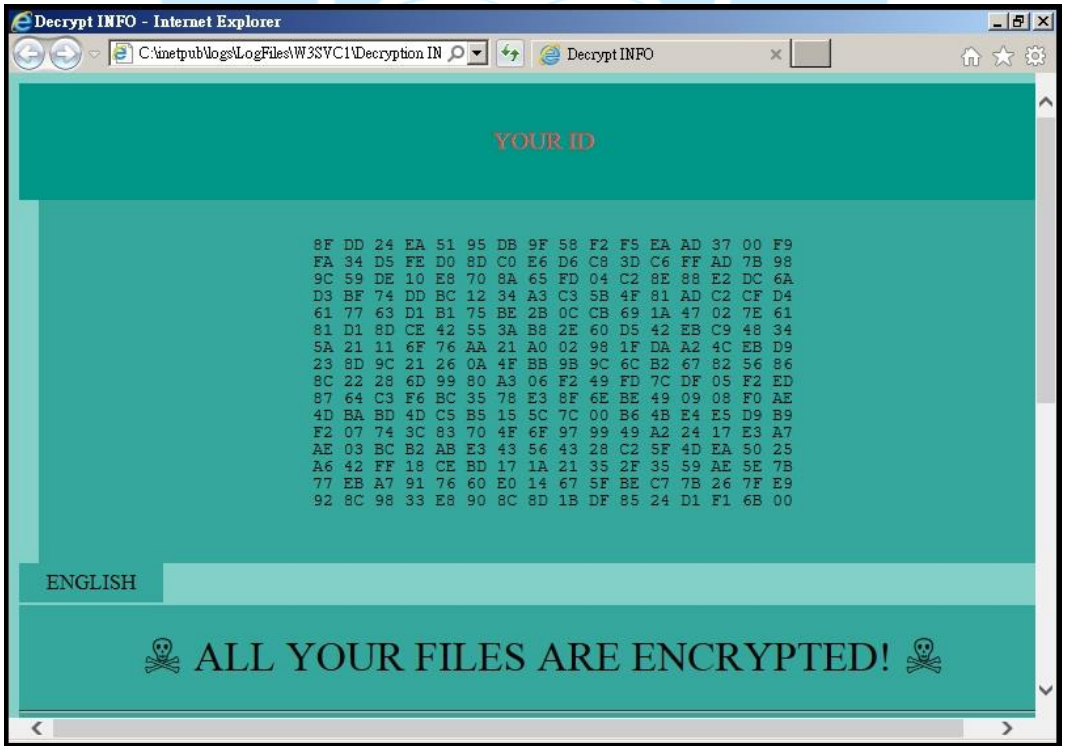
3. 從帳戶 Meixxx 的內容設定發現主機的遠端控制功能是開啟的，並且操控主機的權限層級非「檢視使用者工作階段」，而是設定為「與工作階段互動」。由此設定得知若駭客能從遠端連線入侵主機，則可在主機上執行惡意程式的機率很高。

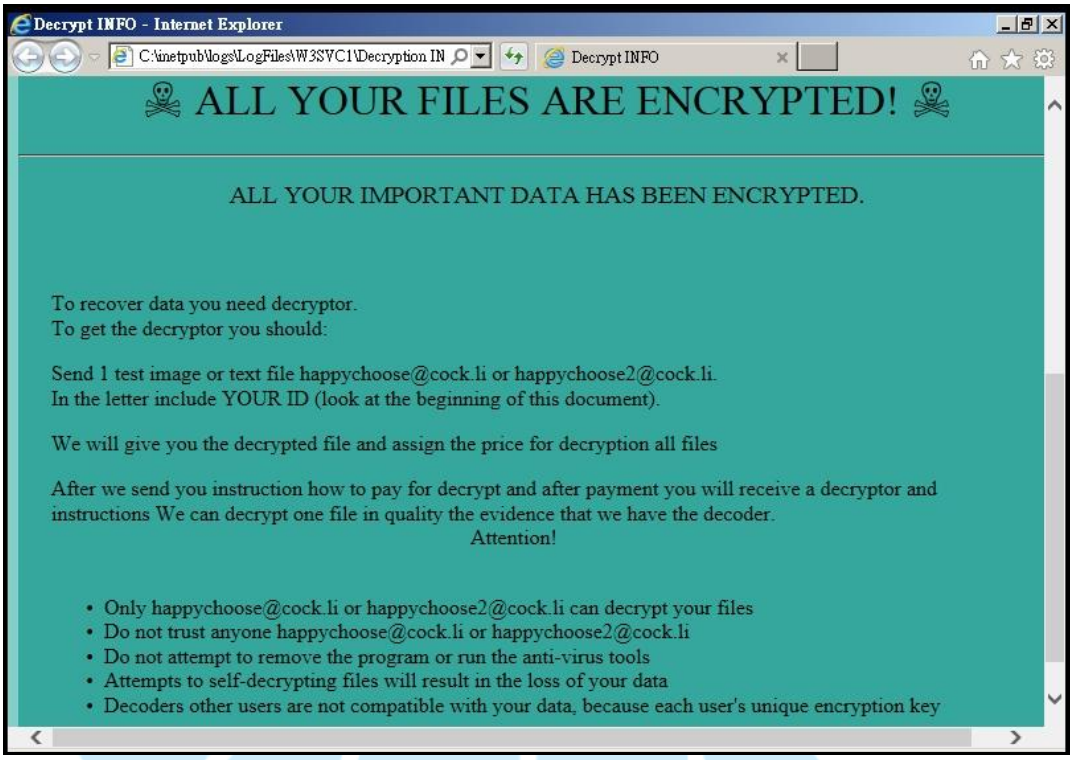


4. 查看主機內檔案狀態發現主機內有被加密的檔案其副檔名皆為 HAPPY4CHOOSE，而且在被加密的資料夾內都會有一個 Decryption INFO.html 檔。



5. 經檢視 Decryption INFO.html 內容，發現其為一個勒索通知信。信中提供受害者 ID，並告訴受害者需有解密器才可以將檔案解密。駭客也告訴受害者可以提供 1 個測試的影像檔或文字檔，附上受害者 ID 寄至 happychoose@cock.li 或 happychoose2@cock.li 信箱。駭客會將該檔案解密後連同解密所有檔案的贖金資訊回傳給受害者。待受害者給付贖金後，駭客會將解密器提供給受害者。





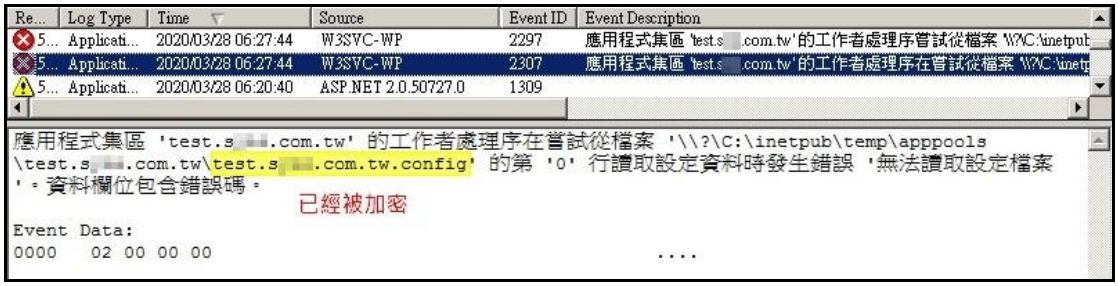
6. 將一個被加密的檔案與勒索通知信 Decryption INFO.html 送 ID Ransomware(https://id-ransomware.malwarehunterteam.com) 勒索病毒辨別網站，經檢測判定為 GlobeImposter 2.0 勒索病毒。

7. 從檔案被加密的時間點得知檔案被加密的時間介於 2020/03/28 05:58~06:28，推測駭客在 2020/03/28 05:58 之前就有駭入主機的行為。

8. 從主機的操作紀錄發現，在檔案將被加密前(2020/03/28 05:58:22)有使用滑鼠點開 C:\Users\Public\Videos 資料夾的紀錄，推測此行為可能為駭客所為。

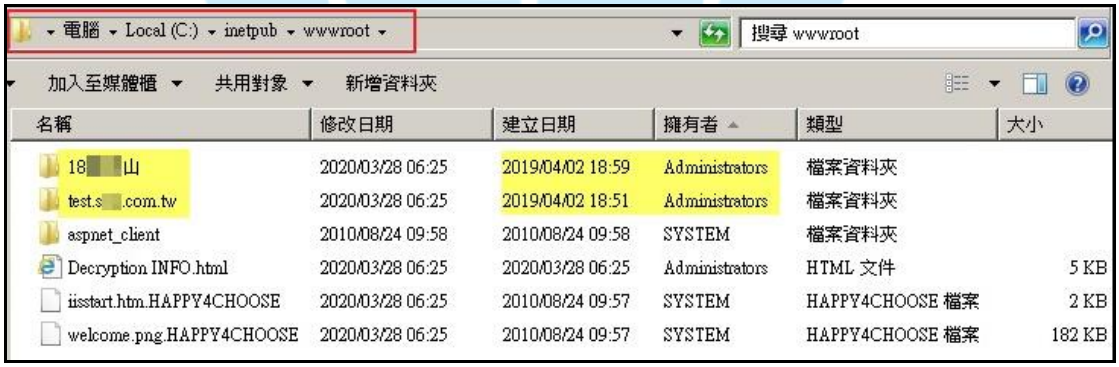
Action Time	Description	Filename	Full Path
2020/03/29 15:22:52	User Logoff		
2020/03/29 15:16:12	User Logon		
2020/03/29 03:03:13	Windows Installer Ended		
2020/03/29 03:01:25	Software Installation		
2020/03/29 03:00:47	Windows Installer Started		
2020/03/28 22:51:44	User Logon		
2020/03/28 20:04:38	User Logon		
2020/03/28 05:58:22	Open file or folder	Videos	C:\Users\Public\Videos
2020/03/21 07:02:12	Software Installation		
2020/03/21 07:02:12	Windows Installer Ended		
2020/03/21 07:02:10	Windows Installer Ended		
2020/03/21 07:02:10	Windows Installer Started		
2020/03/21 07:02:10	Windows Installer Started		

9. 在系統日誌紀錄中發現主機網站 test.sxxx.com.tw 所建立的 temp 資料夾內，有一個 test.sxxx.com.tw 資料夾發生讀取網站 config 錯誤的紀錄，推測可能是因為這些網站資料已被加密，故造成讀取錯誤。



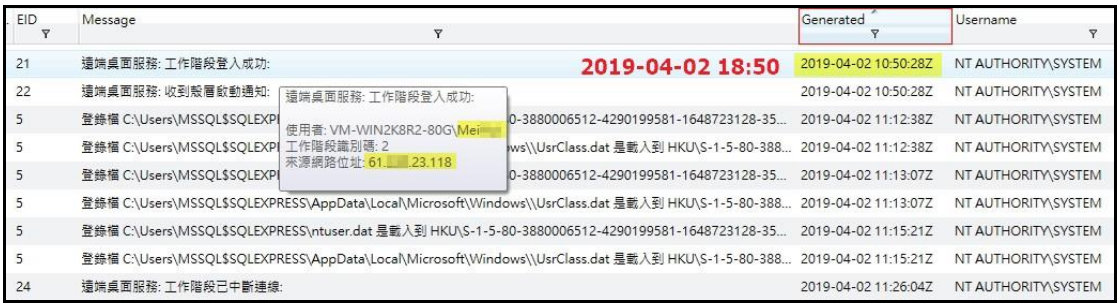
10. C:\inetpub\temp\apppools\test.sxxx.com.tw 內發現上面所提到的檔案 test.sxxx.com.tw.config，它在 2020/01/16 上午 04:24 被 Administrators 群組建立，從建立檔案的日期判斷此行為應該非管理者所為。

11. 在 C:\inetpub\wwwroot 資料夾內發現 2019/04/02 18:51 與 18:59 由 Administrators 群組所建立的兩個網站資料夾「test.sxxx.com.tw」與「18XX 山」，管理者告知「 18XX 山」資料夾為其所建立，而「test.sxxx.com.tw 」 非其所建立，推測「test.sxxx.com.tw」資料夾可能是駭客駭入所建立，因此該主機在一年前可能已經有被駭客駭入的現象。



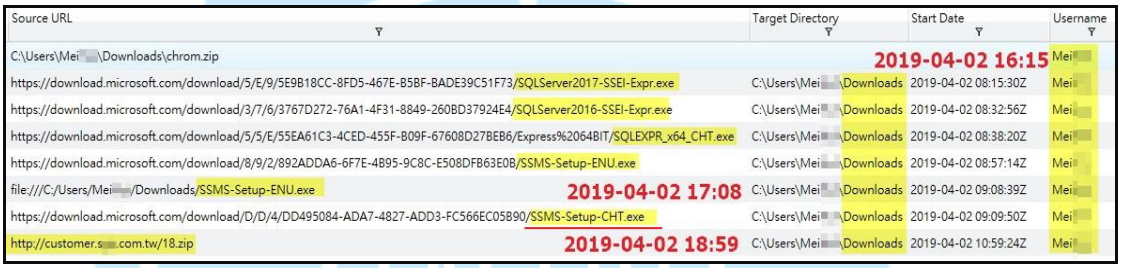
12. 在系統日誌中發現 2019/04/02 18:50~19:26 帳戶 Meixxx 從 IP:61.X.23.118 (中華電信)以遠端桌面方式登入主機。另該帳戶在 2019/04/02 15:50~18:37 期間也從 IP:61.X.23.118 登入主機。

(註:下圖時間為 UTC 時間，需加 8 小時才是台灣時間)

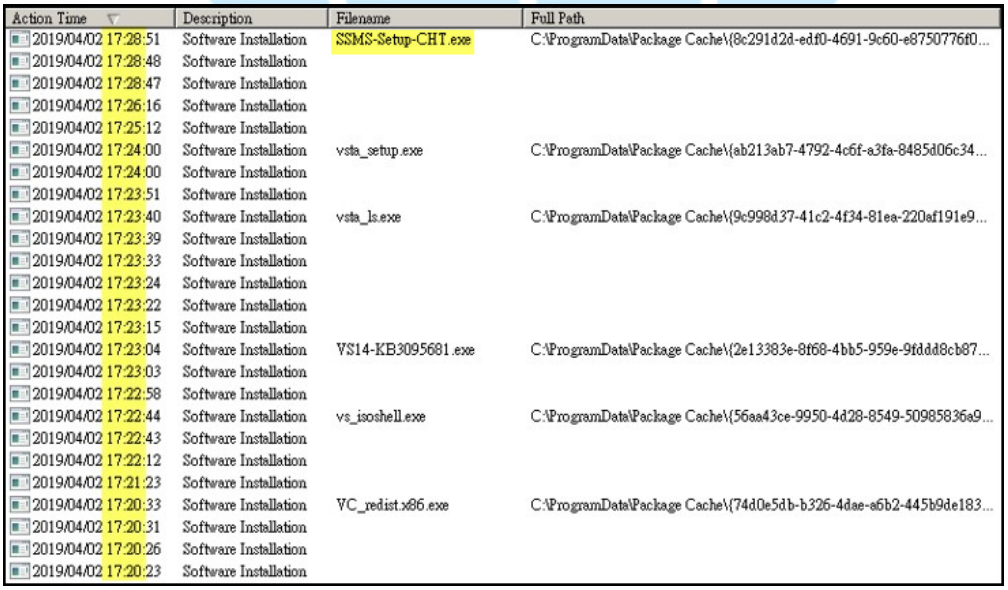


13.檢視 Meixxx 的網頁下載紀錄，發現 Meixxx 在 2019/04/02 16:15 至 18:59 期間曾經下載一些執行檔(含 SSMS-Setup-CHT.exe)，並在 2019/04/02 18:59 從 http://customer.sxxx.com.tw/下載 18.zip。

(註:下圖時間為 UTC 時間，需加 8 小時才是台灣時間)



14.從主機的操作紀錄發現主機在 2019/04/02 16:49-17:28 期間安裝軟體(含 SQL 軟體與 SSMS-Setup-CHT.exe)。又 Meixxx 在 2019-04-02 16:15-17:09 期間曾下載一些執行檔(含 SQL 安裝檔與 SSMS-Setup-CHT.exe)，故推測此軟體安裝行為為 Meixxx 所為。



Action Time	Description	Filename	Full Path
2019/04/02 17:20:23	Software Installation	msiexec.exe	msiexec.exe
2019/04/02 17:20:22	Software Installation		
2019/04/02 17:20:22	Software Installation	msiexec.exe	msiexec.exe
2019/04/02 17:20:19	Software Installation		
2019/04/02 17:20:09	Software Installation		
2019/04/02 17:20:04	Software Installation		
2019/04/02 17:20:01	Software Installation		
2019/04/02 17:19:56	Software Installation		
2019/04/02 17:19:48	Software Installation		
2019/04/02 17:19:20	Software Installation		
2019/04/02 17:18:51	Software Installation		
2019/04/02 17:18:47	Software Installation		
2019/04/02 17:18:47	Software Installation		
2019/04/02 17:18:35	Software Installation		
2019/04/02 17:18:30	Software Installation		
2019/04/02 17:18:27	Software Installation		
2019/04/02 17:18:22	Software Installation		
2019/04/02 17:18:19	Software Installation		
2019/04/02 17:18:06	Software Installation		
2019/04/02 17:18:01	Software Installation		
2019/04/02 17:17:58	Software Installation		
2019/04/02 17:17:56	Software Installation	VC_redist.x64.exe	C:\ProgramData\Package Cache\{e46eca4f-393b-40df-9f49-076faf788d8...
2019/04/02 17:17:51	Software Installation	vcredist_x64.exe	C:\ProgramData\Package Cache\{4e7db4cc-d429-40c4-b359-bcc70debf7...
2019/04/02 17:17:46	Software Installation	vcredist_x86.exe	C:\ProgramData\Package Cache\{e5bb5c4d-7276-4254-8320-5a976f34e0...
2019/04/02 17:17:45	Software Installation		

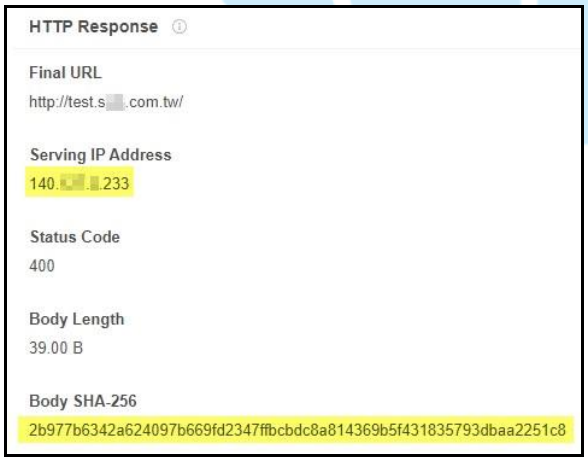
Action Time	Description	Filename	Full Path	More Information
2019/04/02 17:17:44	Software Installation			Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005
2019/04/02 17:16:56	Software Installation			SQL Server 2017 Common Files
2019/04/02 17:16:49	Software Installation			SQL Server 2017 Common Files
2019/04/02 17:16:48	Software Installation			Microsoft SQL Server 2017
2019/04/02 17:16:48	Software Installation			Microsoft SQL Server 2017
2019/04/02 17:16:42	Software Installation			Microsoft Analysis Services OLE DB 提供者
2019/04/02 17:15:12	Software Installation			Microsoft SQL Server 2017 原則
2019/04/02 17:15:09	Software Installation			Microsoft SQL Server Data-Tier Application Framework (x86) - zh-...
2019/04/02 17:14:53	Software Installation			Microsoft Visual C++ 2015 x86 Additional Runtime - 14.0.23026
2019/04/02 17:14:51	Software Installation			Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.0.23026
2019/04/02 16:50:17	Software Installation			適用於 SQL Server 2014 的 SQL Server Browser
2019/04/02 16:49:28	Software Installation			Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2549743
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2524860
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2565063
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2544655
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB982573
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2151757
2019/04/02 16:49:28	Software Installation			{F0C3E5D1-1ADE-321E-8167-68EF0DE699A5}.KB2467173
2019/04/02 16:49:25	Software Installation			{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2565063
2019/04/02 16:49:25	Software Installation			{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2549743
2019/04/02 16:49:25	Software Installation			{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2524860
2019/04/02 16:49:25	Software Installation			{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2544655
2019/04/02 16:49:25	Software Installation			{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB982573
2019/04/02 16:49:25	Software Installation			{1D8E6291-B0D5-35EC-8441-6616F567A0F7}.KB2151757

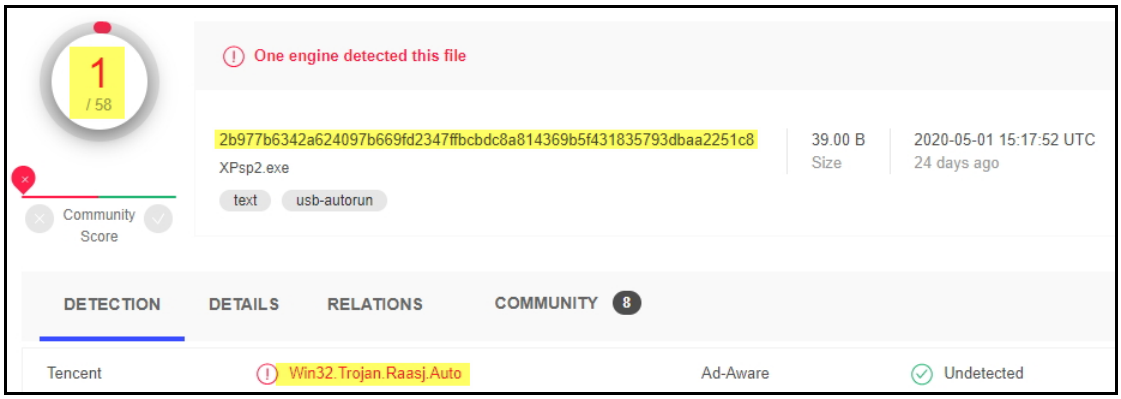
15.從 Meixxx 的網頁瀏覽紀錄，發現 Meixxx 在 2019/04/02 18:54 開始陸續連線 http://test.sxxx.com.tw，疑似在測試 test.sxxx.com.tw 網站。

Visit Type	URL		Last Visit Date	Username
URL			2019-04-02 10:51:36Z	Mei
URL	file:///C:/inetpub/wwwroot/test.s[redacted].com.tw/index.htm	2019/04/02 18:54	2019-04-02 10:54:33Z	Mei
Link	http://test.s[redacted].com.tw/		2019-04-02 10:54:38Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 10:54:50Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 10:54:51Z	Mei
Reload	http://test.s[redacted].com.tw/	2019/04/02 18:55	2019-04-02 10:55:11Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 10:55:13Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 10:55:17Z	Mei
URL	file:///C:/Users/Mei[redacted]/Downloads/18.zip	2019/04/02 18:59	2019-04-02 10:59:46Z	Mei
URL			2019-04-02 11:01:12Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 11:01:55Z	Mei
URL	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityLi...		2019-04-02 11:03:24Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 11:06:54Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 11:07:19Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 11:15:49Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 11:15:55Z	Mei
Reload	http://test.s[redacted].com.tw/		2019-04-02 11:16:46Z	Mei

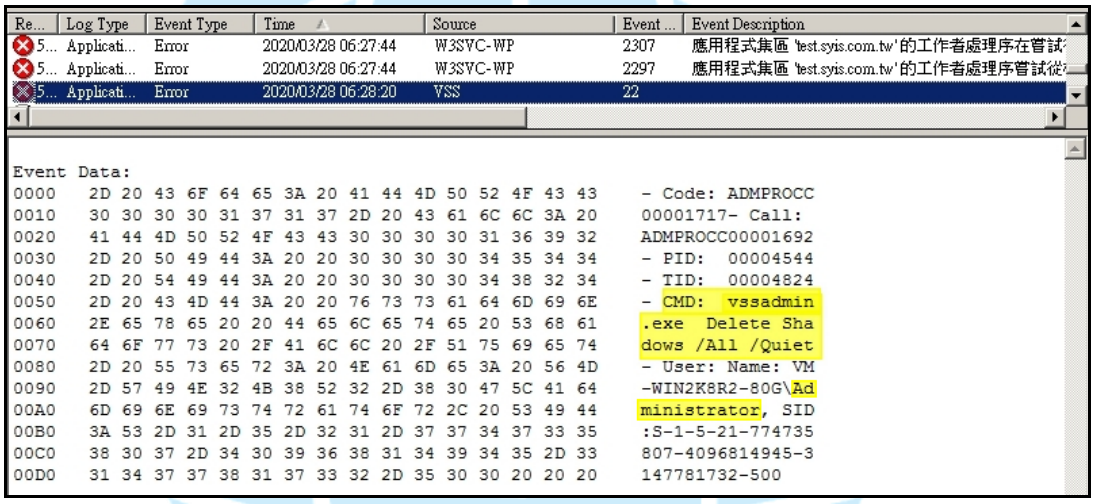
16. 在 C:\inetpub\temp\...\WWWROOT 資料夾內發現由「test.sxxx.com.tw」在 2019/04/08 14:14 所建立的「18XX 山」資料夾，推測該資料夾是解壓縮後產生「18XX 山」網站的資料夾。由此可以得知駭客透過「test.sxxx.com.tw」網站取得「18XX 山」的網站資料。

17. 透過 Virustotal 檢視網址 test.sxxx.com.tw 的惡意程度，發現該網址對應 IP 為 140.X.X.233(為本主機的 IP)，其惡意比例為 0/79，而且該網址曾有一個惡意程式提供下載。查看該惡意程式的惡意比例為 1/58，僅一家防毒軟體認為其為惡意程式。在 Virustotal 的資安社群中討論其為透過 USB 傳播的病毒。由這些資訊推測本主機的網站可能為駭客駭入主機所架設，而非管理者所建立。

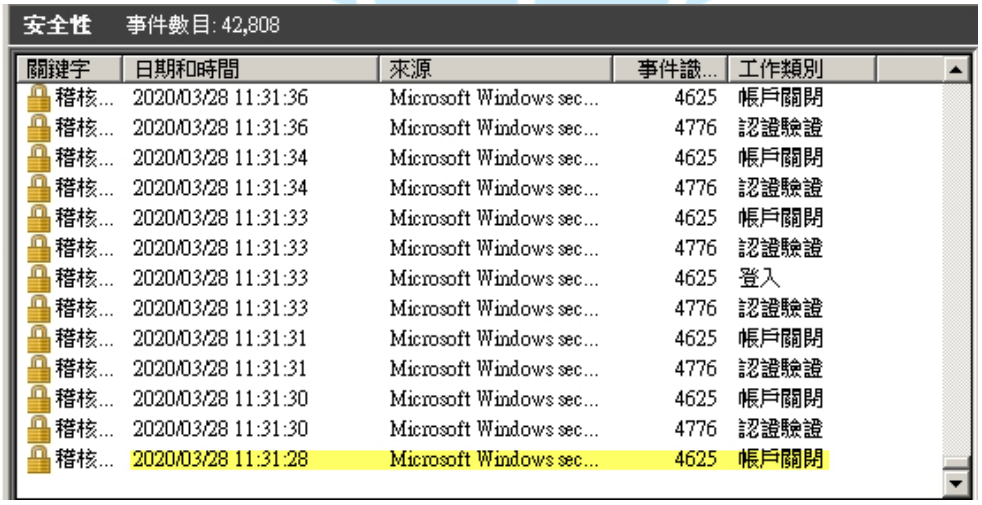




18. 由主機的系統日誌發現在 2020/03/28 06:28 主機檔案被加密的過程中，駭客以帳戶 Administrator 登入，並執行「vssadmin.exe Delete Shadows /All /Quiet」刪除影子副本的指令。



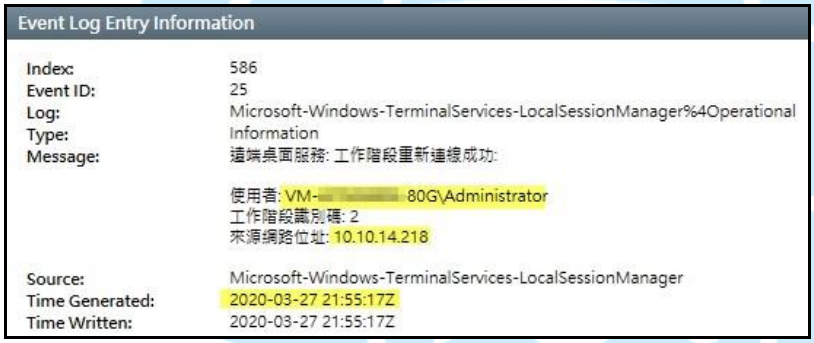
19. 檢視主機內事件檢視器的安全性紀錄得知在 2020/03/28 11:31 之前的紀錄已不存在，但是其他類別的紀錄仍存在，推測此紀錄可能是被駭客刪除。



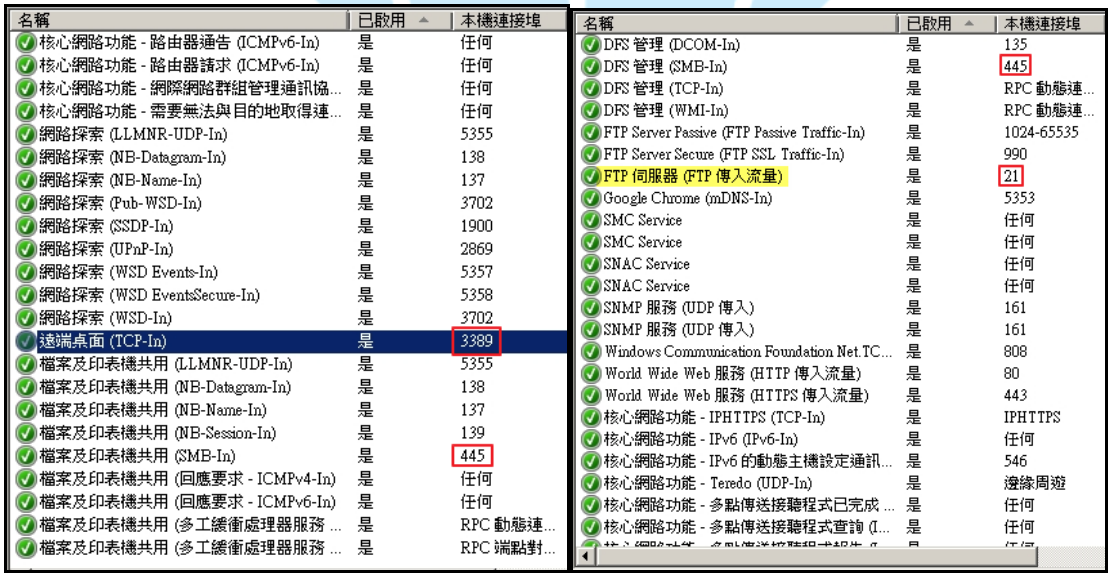
20.從主機的各帳戶登入紀錄發現，在 2020/03/28 有 6 筆帳戶 Administrator 以遠端桌面或網路方式登入主機的紀錄，其中以 IP:10.10.14.218 在 2020/03/28 5:55 登入主機的時間點最接近檔案開始被加密的時間 5:58。

Logon Time	User Name	IP	Logon Type
2020/03/28 2:47	Administrator	10.10.14.100	10(遠端桌面)
2020/03/28 5:55	Administrator	10.10.14.218	10(遠端桌面)
2020/03/28 19:48:50	Administrator	10.10.14.19	3(網路登入)
2020/03/28 19:48:56	Administrator	140.X.X.19	3(網路登入)
2020/03/28 20:04	Administrator	10.10.14.100	10(遠端桌面)
2020/03/28 22:51	Administrator	140.X.X.28	10(遠端桌面)

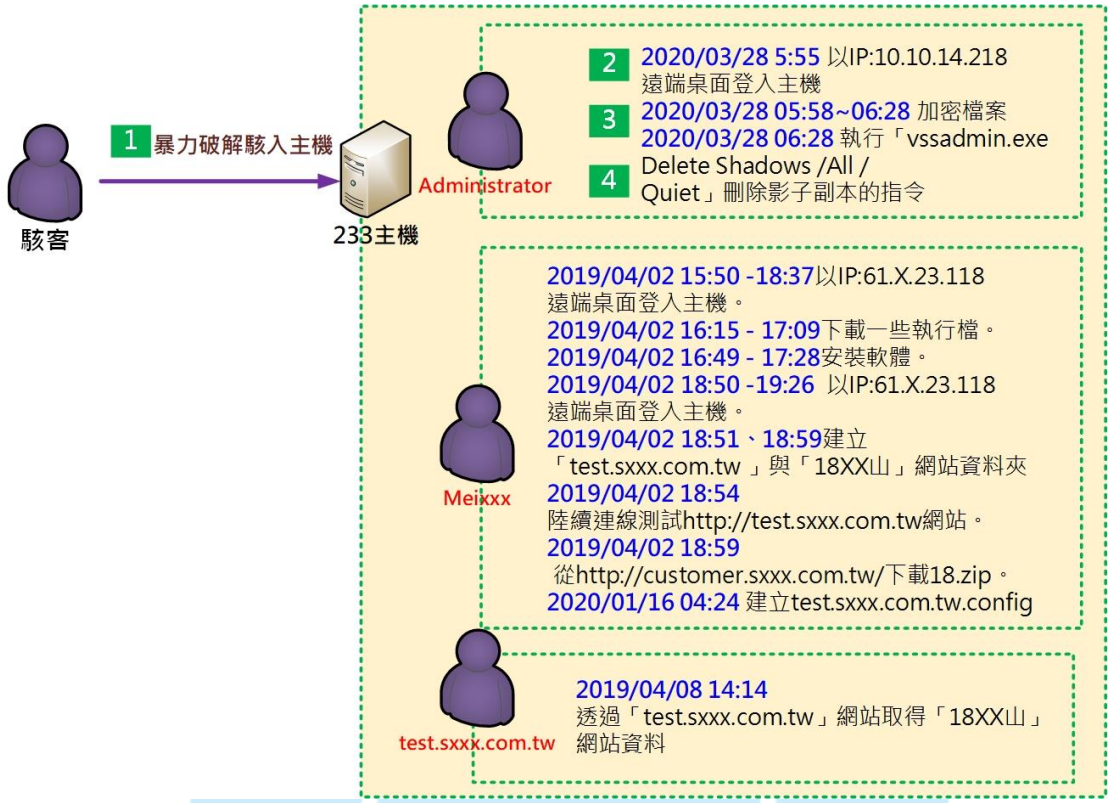
(註:下圖時間為 UTC 時間，需加 8 小時才是台灣時間)



21.檢視該主機對外所開啟的port狀態，發現該主機開啟駭客常會攻擊的3389port與 445port，也開啟 FTP 所使用的 21port。此行為容易造成主機被駭客攻擊。



三、事件攻擊行為示意圖



雖然受害主機在一年前就有駭客駭入足跡，但本事件的檢測目的主要是探討受害主機如何感染 GlobeImposter 2.0 勒索病毒的過程，故在此將針對此疑問進行說明如下。

1. 駭客以暴力破解方式駭入主機。
2. 駭客從 IP:10.10.14.218 以遠端桌面方式登入受害主機。(2020/03/28 05:55)
3. 駭客對受害主機內的檔案進行加密作業。(2020/03/28 05:58~06:28)
4. 在加密作業完成後執行刪除影子副本的指令。(2020/03/28 06:28)

四、總結與建議

1. 本事件為學校在 2020/03/28 當日多台主機同時感染勒索病毒，從學校所提供的檢測主機上發現當日有一個 IP:10.10.14.218 以帳戶 Administrator 登入

主機，之後該主機即有檔案被加密的現象發生。

2. 在受害主機上發現「test.sxxx.com.tw」與「18XX 山」網站資料夾在 2019/04/02 18:51 與 18:59 被 Administrators 群組所建立，而「test.sxxx.com.tw」非管理者或使用者所建立。在同天 18:54 被帳戶 Meixxx 以網頁瀏覽方式陸續存取 test.sxxx.com.tw 網站，疑似為駭客駭入主機後所為，推測該主機在一年前已經被駭客駭入。
3. 該受害主機有開啟一些駭客常會攻擊的 port (21、3389、445Port)，其中 445port 為勒索病毒常用來散播病毒的管道。如無特殊需求，建議關閉 445port 的服務。
4. 該受害主機經檢測是感染 GlobeImposter 2.0 勒索病毒。該病毒在執行後通常會自己從所在的資料夾中消失，無法搜尋到它的存在之處。目前該病毒沒有解密器，建議將已被加密的重要檔案備份，等待未來有解密器產生時進行解密。
5. 在預防勒索病毒方面，有下列建議作法提供參考。
   (1)定期進行作業系統、應用程式與防毒軟體病毒碼的更新。
   (2)定期清查重要資料，並定期進行資料備份作業。
   (3)檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要的使用與存取。
   (4)定期檢視作業系統與應用程式更新紀錄，避免駭客利用作業系統或應用程式的安全性漏洞進行入侵行為。
   (5)當使用隨身碟傳輸資料時，應先檢查隨身碟是否感染病毒或惡意程式。
   (6)如非必要盡量減少使用網路磁碟機來共享資料，以降低勒索病毒擴散的風險。
   (7)定期檢視主機 port 開啟的狀況，如無需求可關閉勒索軟體常會使用來散播病毒的 445port，也盡量減少開啟遠端桌面連線會使用的 3389port。
   (8)平時應加強校內人員的教育訓練，提升使用者對勒索軟體的知識。讓

使用者平時即留意收發的電子郵件是否安全，並且注意郵件來源的正確性。養成使用者不隨意開啟不明來源信件的附檔或連結的習慣，以防感染惡意程式。

6. 當主機疑似感染勒索軟體時，有下列應對措施提供參考。

(1)發現當下應立即關閉主機並切斷網路，避免災情擴大。

(2)立即通知資訊人員或廠商協助搶救還沒被加密的檔案。

(3)對於已被加密的檔案，可保留一份備份，以待未來有解密器時可還原檔案。

(4)建議重新安裝作業系統與應用程式，並確認已安裝至最新修補程式後，再還原備份的資料。

(5)備份資料在還原至主機之前，應以防毒軟體檢查主機，確保沒有殘存的惡意程式於主機內。

(6)待還原備份的資料至重新安裝的主機後，進行資料盤點與確認是否有資料遺失的狀況。