**TLP:WHITE**

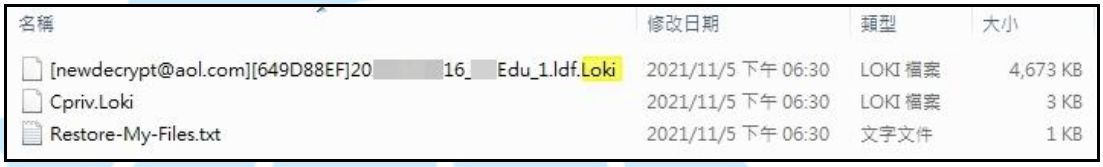
# 勒索病毒 Loki Locker 分析報告

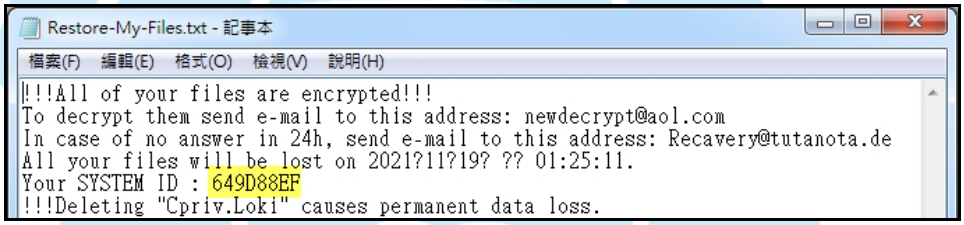
**臺灣學術網路危機處理中心團隊(TACERT)製**

**2021 年 12 月**

# 一、事件簡介

1. 在 2021/11 初某單位所管理轄下學校之共構網站資料庫系統主機，被駭客透過該單位所新建測試主機入侵後感染勒索病毒，造成轄下 185 所國中小學網站無法瀏覽。
2. TACERT 協助該單位判別勒索病毒的種類，而由該單位所提供之資料判定感染 Loki Locker 之變種病毒。被加密過檔案之檔名會被更改為下列結構:[聯絡信箱][SYSTEM ID]原檔案名稱.Loki。
3. 該病毒執行後會產生 Cpriv.Loki 與 Restore-My-Files.txt (Ransom Note) 。

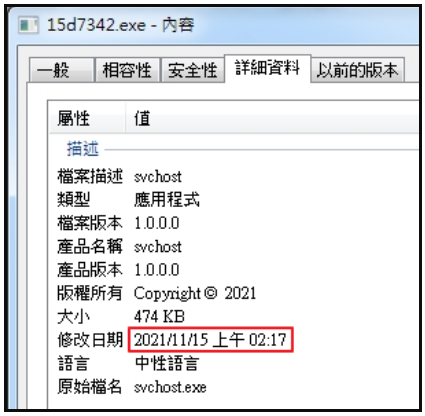



4. 為進一步了解該勒索病毒的特徵與其攻擊行為，TACERT 對該病毒樣本進行分析。

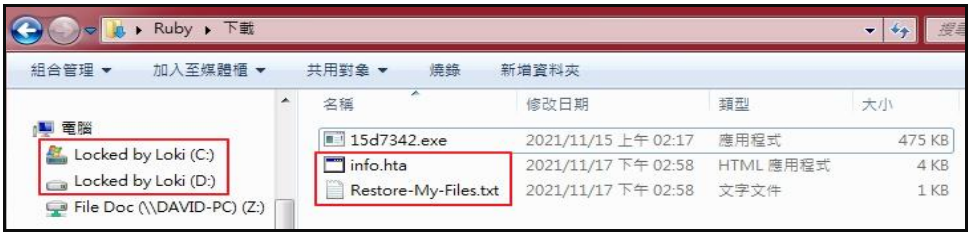
# 二、事件檢測

1. 在 Windows 7 32 位元的系統上執行病毒樣本 15d7342.exe (MD:8aea251877cb4f5ee6cf357831f8620c)。

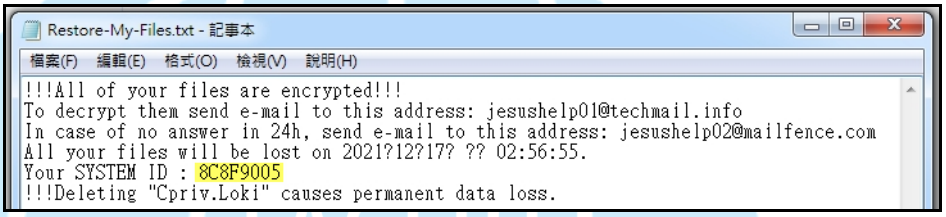


(1) 執行後 C、D 磁碟機名稱會被更名為「Locked by Loki」，網路磁碟機不受影響。

(2) 產生 info.hta 與 Restore-My-Files.txt 於病毒樣本所在資料夾中。




(3) Restore-My-Files.txt 告訴受害者所有檔案已被加密，若要解密需 24 小時內寫信至聯絡信箱，否則檔案會在到期時間後遺失。也告訴受害者 SYSTEM ID 與不要刪除 Cpriv.Loki，以免檔案遺失。




2. 在加密作業完成後會執行 5 個 info.hta 腳本，這些 info.hta 為 Ransom note(勒索通知信)。它提供兩個聯絡信箱、受害主機 ID 與繳款期限等資訊，也告知受害者需 48 小時內聯絡或付款，而且 1 個月後檔案會遺失。

3. 在桌面上會看到 Loki locker 的紅字文，內容與 info.hta 相似。它告訴受害者在每個被加密的資料夾中都有 Restore-My-Files.txt 提供參考。


4. 檢視對外網路連線情形，發現會連線荷蘭 IP:91.223.82.6:80。從側錄封包上得知此行為類似連線報到，並無傳送任何惡意程式或檔案。

| | | | |
|---|---|---|---|
| 2021/11/17 下午 02:56:41 Added | svchost.exe | UDP 0.0.0.0:56228 | *:* |
| 2021/11/17 下午 02:56:43 Added | 15d7342.exe | TCP 192.168.137.135:49224 | 91.223.82.6:80 |

5. 查看 Cpriv.Loki 內容為一大段亂碼，該檔案會在每次病毒執行後產生新的亂碼內容。

(1) 檢測主機首次執行病毒，Cpriv.Loki 內容如下圖。


(2) 檢測主機重新開機後，Cpriv.Loki 內容如下圖。


6. 檢視 15d7342.exe 執行後呼叫程式的情形，發現可以分為三個部分。

| Process | Command |
|---|---|
| 15d7342.exe (3828) | "C:\Users\Ruby\Downloads\15d7342.exe" |
| cmd.exe (3684) | "C:\Windows\System32\cmd.exe" /C schtasks /CREATE /SC ONLOGON /TN Loki /TR C:\Users\Ruby\AppData\Roaming\winlogon.exe /RU SYSTEM /RL HIGHEST /F |
| schtasks.exe (3368) | schtasks /CREATE /SC ONLOGON /TN Loki /TR C:\Users\Ruby\AppData\Roaming\winlogon.exe /RU SYSTEM /RL HIGHEST /F |
| csc.exe (1132) | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\Ruby\AppData\Local\Temp\yqiudgft.cmdline" |
| cvtres.exe (3888) | C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\Ruby\AppData\Local\Temp\RES5457.tmp" "c:\ProgramData\CSCDCE7D0B7D8644D58BB1313D6187D5521.TMP" |
| 15d7342.exe (1708) | "C:\Users\Ruby\Downloads\15d7342.exe" |
| csc.exe (3508) | "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\Ruby\AppData\Local\Temp\ka2wid3i\ka2wid3i.cmdline" |
| cvtres.exe (2904) | C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\Ruby\AppData\Local\Temp\RESA277.tmp" "c:\ProgramData\CSC1C0CBC952263446EBBA6C812DEAD9D.TMP" |
| cmd.exe (1828) | "C:\Windows\System32\cmd.exe" /C vssadmin delete shadows /all /quiet |
| vssadmin.exe (1964) | vssadmin delete shadows /all /quiet |
| cmd.exe (1028) | "C:\Windows\System32\cmd.exe" /C wbadmin DELETE SYSTEMSTATEBACKUP |
| wbadmin.exe (2032) | wbadmin DELETE SYSTEMSTATEBACKUP |
| cmd.exe (2400) | "C:\Windows\System32\cmd.exe" /C wmic shadowcopy delete |
| WMIC.exe (3876) | wmic shadowcopy delete |
| cmd.exe (3280) | "C:\Windows\System32\cmd.exe" /C wbadmin delete catalog -quiet |
| wbadmin.exe (3216) | wbadmin delete catalog -quiet |
| cmd.exe (3784) | "C:\Windows\System32\cmd.exe" /C bcdedit /set {default} bootstatuspolicy ignoreallfailures |
| bcdedit.exe (1560) | bcdedit /set {default} bootstatuspolicy ignoreallfailures |
| cmd.exe (956) | "C:\Windows\System32\cmd.exe" /C bcdedit /set {default} recoveryenabled no |
| bcdedit.exe (2220) | bcdedit /set {default} recoveryenabled no |
| cmd.exe (1104) | "C:\Windows\System32\cmd.exe" /C netsh advfirewall set currentprofile state off |
| netsh.exe (2004) | netsh advfirewall set currentprofile state off |
| cmd.exe (1148) | "C:\Windows\System32\cmd.exe" /C netsh firewall set opmode mode=disable |
| netsh.exe (3772) | netsh firewall set opmode mode=disable |
| mshta.exe (984) | "C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Downloads\info.hta" |
| mshta.exe (2460) | "C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Downloads\info.hta" |
| mshta.exe (3000) | "C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Downloads\info.hta" |
| mshta.exe (2036) | "C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Downloads\info.hta" |
| mshta.exe (3444) | "C:\Windows\System32\mshta.exe" "C:\Users\Ruby\Downloads\info.hta" |

15d7342.exe 執行後:

(1) 呼叫 cmd.exe 執行 schtasks.exe 來建立登入自動執行之新排程 Loki ，該排程使用本機系統帳戶的最高權限執行 winlogon.exe。

winlogon.exe 位於使用者帳戶的 AppData\Roaming 內，被視為作業系

統檔案而隱藏。

(2) 呼叫 csc.exe 執行 cvtres.exe 來修復因 Compiler 發生錯誤、無法執行程式所造成的執行階段錯誤。

(3) 再次呼叫 15d7342.exe 來執行下列程式

(3.1) 呼叫 csc.exe 來執行 cvtres.exe。

因 Compiler 發生錯誤、無法執行程式。透過 cvtres.exe 來修復執行階段錯誤。

(3.2) 呼叫 cmd.exe。

(3.2.1)執行 vssadmin.exe 刪除所有指定磁碟區的陰影複製(在執行時，命令不會顯示訊息)。

(3.2.2)執行 wbadmin.exe 刪除一或多個系統狀態備份。

(3.2.3)執行 WMIC.exe 來刪除影子副本。

(3.2.4)執行 wbadmin.exe 刪除本機電腦上的備份類別目錄。

(3.2.5)執行 bcdedit.exe 不顯示 Windows 不正常關機之自動修復訊息。

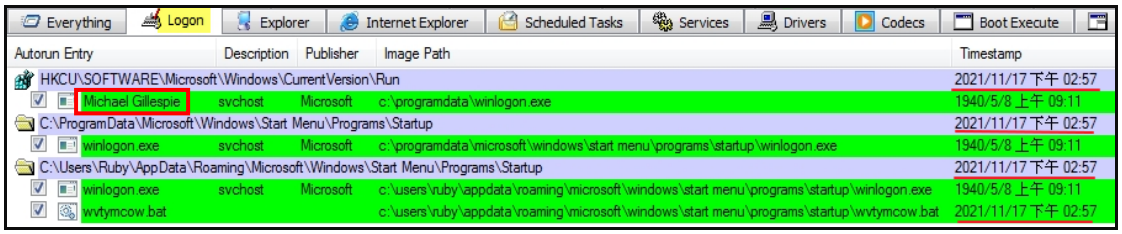
(3.2.6)執行 bcdedit.exe 不顯示不正常斷電時的復原畫面。

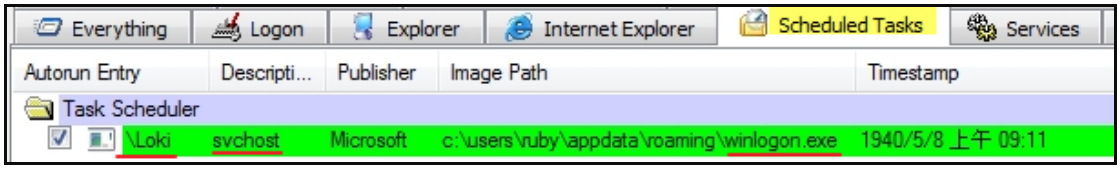
(3.2.7)執行 netsh.exe 關閉"當前"使用的防火牆。

(3.2.8)執行 netsh.exe 停用防火牆。

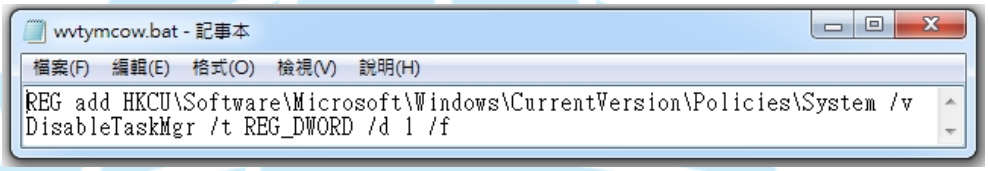
(3.3)執行 5 個 mshta.exe 來執行 info.hta 腳本，以開啟勒索通知信的畫面。

7. 從開機啟動程式內容發現 winlogon.exe 與 wvtymcow.bat 在開機後會自動啟動，而且有建立一個新的 Loki 排程來執行 winlogon.exe。在登錄檔新增的 Michael Gillespie 啟動設定，該名稱是一名勒索軟體研究員的名字，而該研究員分析勒索軟體，以便為勒索軟體受害者建立免費解密器。 他還是 ID Ransomware 服務的建立者，該服務可用於識別受害者感染了哪些勒索軟體。在此 Loki locker 以該研究員名字命名啟動設定之用意耐人尋味。

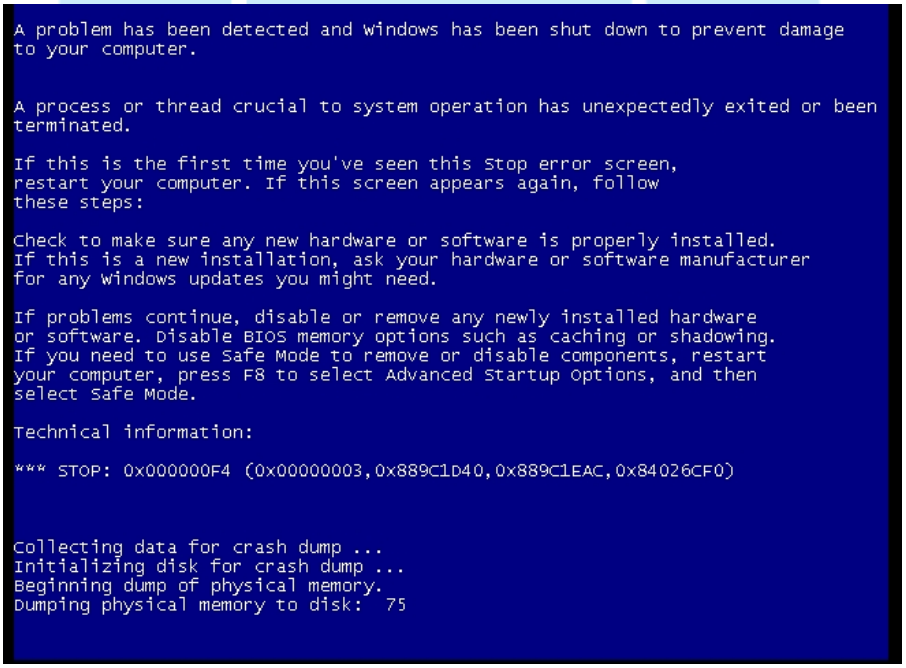


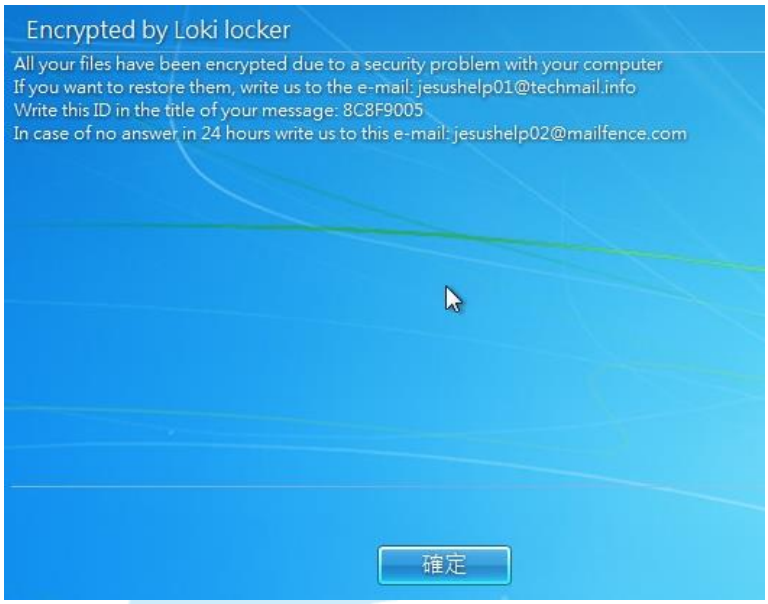




8. 在啟動資料夾中發現新產生的 wvtymcow.bat，其作用是使用系統管理員權限停用任務管理器。wvtymcow.bat 在主機上出現在兩個地方:使用者 appdata 內與 windows\system32 內。

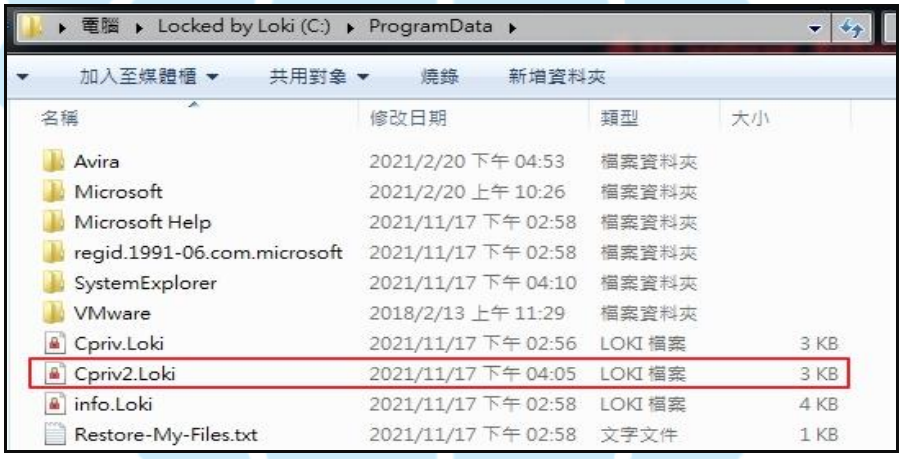



9. 重新開機時，會出現 Blue Screen。之後在系統登入時出現 Encrypted by Loki locker 的資訊。

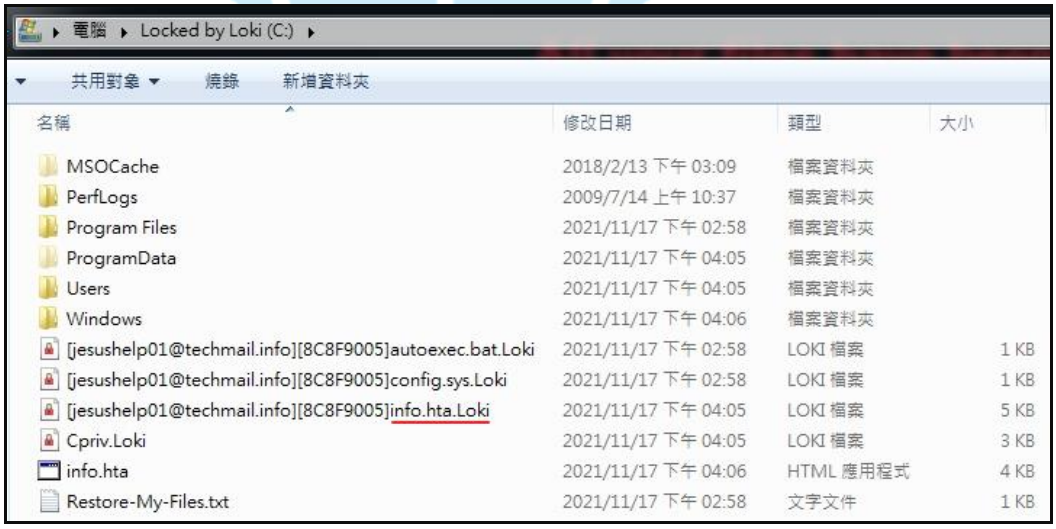




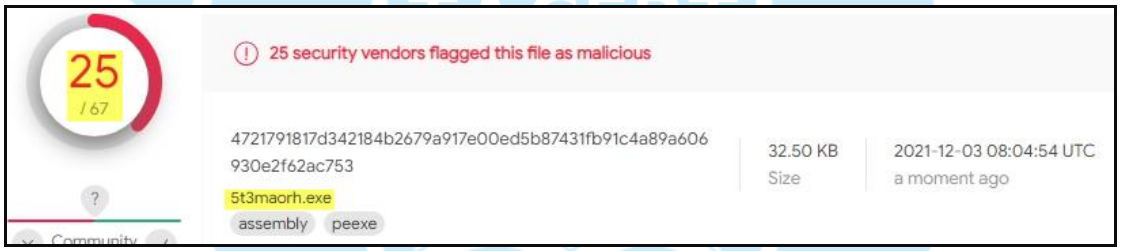

10. 開機完成後 winlogon.exe 啟動，主機再次執行加密作業，之後在 C:\ProgramData 產生 Cpriv2.Loki。

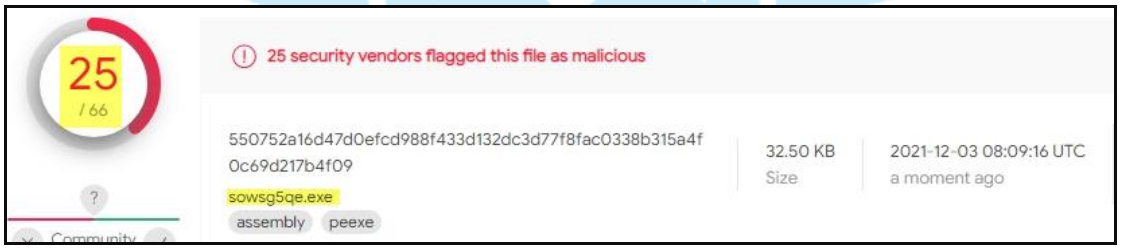



11. 原開機前存在的腳本 info.hta，在重新開機後會被加密。

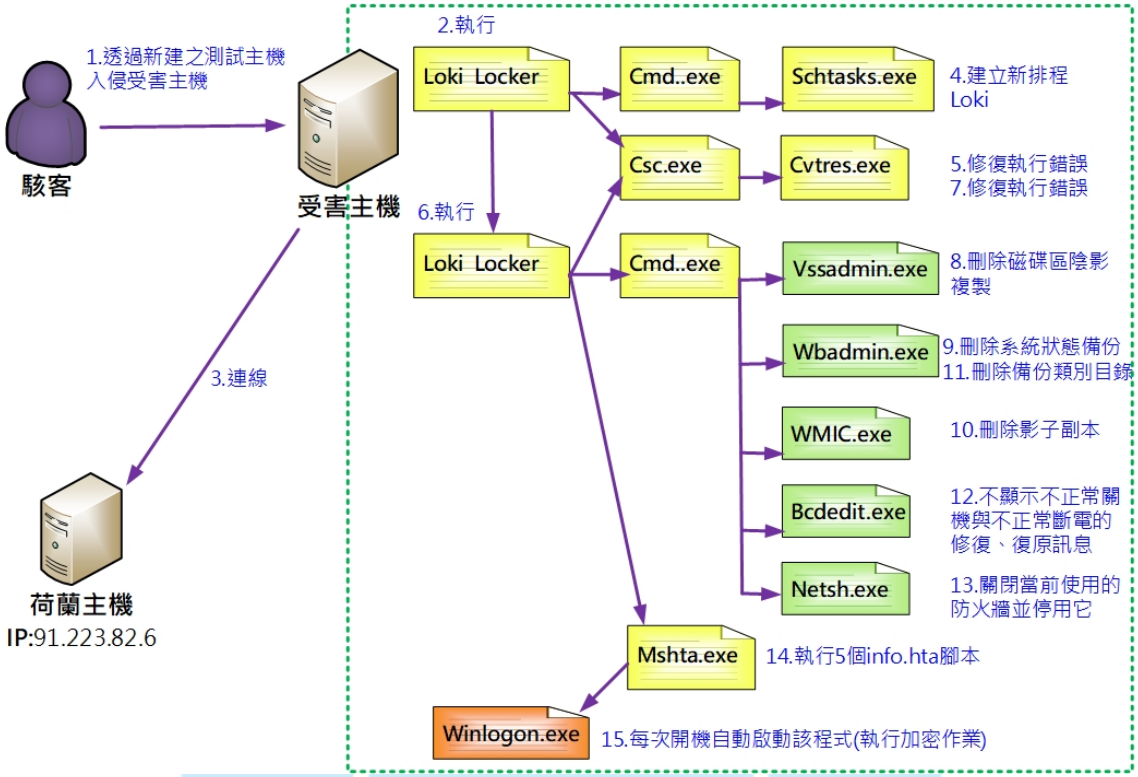


12. 在 C:\ProgramData 發現 3 個偽裝成系統檔的隱藏程式 5t3maorh.exe、sowsg5qe.exe 與 winlogon.exe。經 virustotal 檢測它們惡意比例為 25/67、25/66 與 55/68。這 3 個檔案被 ESET-NOD32 防毒軟體判定為「A Variant of MSIL/Filecoder.LokiLocker.C」，為勒索軟體 LokiLocker 的變種。其中 winlogon.exe 為本案病毒樣本的副本，而其餘兩個檔案為執行過程中產生於主機內的惡意程式。


## 三、攻擊行為示意圖




1.透過新建之測試主機入侵受害主機。

2.執行 157342.exe 開始加密作業。

3.連線荷蘭 IP。

4.建立登入後自動執行之新排程 Loki，讓排程 Loki 以系統管理者權限執行 winlogon.exe，並且自動執行 wvtymcow.bat。

5.修復 Compiler 所造成的執行階段錯誤。

6.再次執行 157342.exe。

7.修復 Compiler 所造成的執行階段錯誤。

8.執行 vssadmin.exe 刪除所有指定磁碟區的陰影複製。

9.執行 wbadmin.exe 刪除一或多個系統狀態備份。

10.執行 WMIC.exe 刪除影子副本。

11.執行 wbadmin.exe 刪除本機電腦上的備份類別目錄。

12.執行 bcdedit.exe 不顯示 Windows 不正常關機的自動修復訊息，以及不顯示不正常斷電時的復原畫面。

13.執行 netsh.exe 關閉「當前」使用的防火牆與停用防火牆。

14.執行 5 個 mshta.exe 來執行 info.hta 腳本。

15.每次開機會啟動 winlogon.exe 來執行加密作業。

(註: winlogon.exe 之 hash 值與 157342.exe 相同。)

## 四、總結與建議

1. 本案所感染的勒索病毒 Loki Locker 是該病毒的新變種，在檢測時該病毒在 ID Ransomware 之勒索軟體識別網站上，還無法使用 Ransom Note 與被加密的檔案來判別出感染它。
2. 它在完成加密過程後，會透過提供三種不同的 Ransom note 來確保受害者必定收到通知。一條訊息將顯示為新的桌面背景圖片，另一條訊息將放置在名為「Restore-My-Files.txt」的文件檔中，而第三組訊息說明將執行 info.hta 顯示在彈出視窗中。此手法與一般勒索病毒只使用一種 Ransom note 不同。
3. 它會將本機磁碟機更名為 Locked by Loki，而且不會加密網路磁碟機內的檔案。此點與一般的勒索病毒特性也不同。
4. 它執行後刪除備份、影子副本、備份類別目錄，不顯示不正常關機或不正常斷電時會彈跳出的復原訊息，以及禁用防火牆功能等動作，完整地呈現一般惡意程式對受害主機會使用的攻擊手法。
5. 該勒索病毒在重新開機後，會自動執行 winlogon.exe 來再次加密主機內的檔案。故在處理受害主機時，需先刪除 winlogon.exe 才可中止惡意程式執行。

6. 本案源起於該單位新建立之測試主機被駭客入侵後，進而在內網中攻擊受害主機，最後導致主機感染 Loki Locker。因此，建議在內網中可採用依用途或需求分類之切割網段方式，以確保各網段的安全。對於執行重要業務之伺服器，建議勿與測試用主機放於相同網段中。
7. 對於勒索病毒 Loki Locker 的預防，建議平時做好定期備份，以免如本案發生時，無法利用備份還原各校網站版型，只能使用公版版型重設網站。