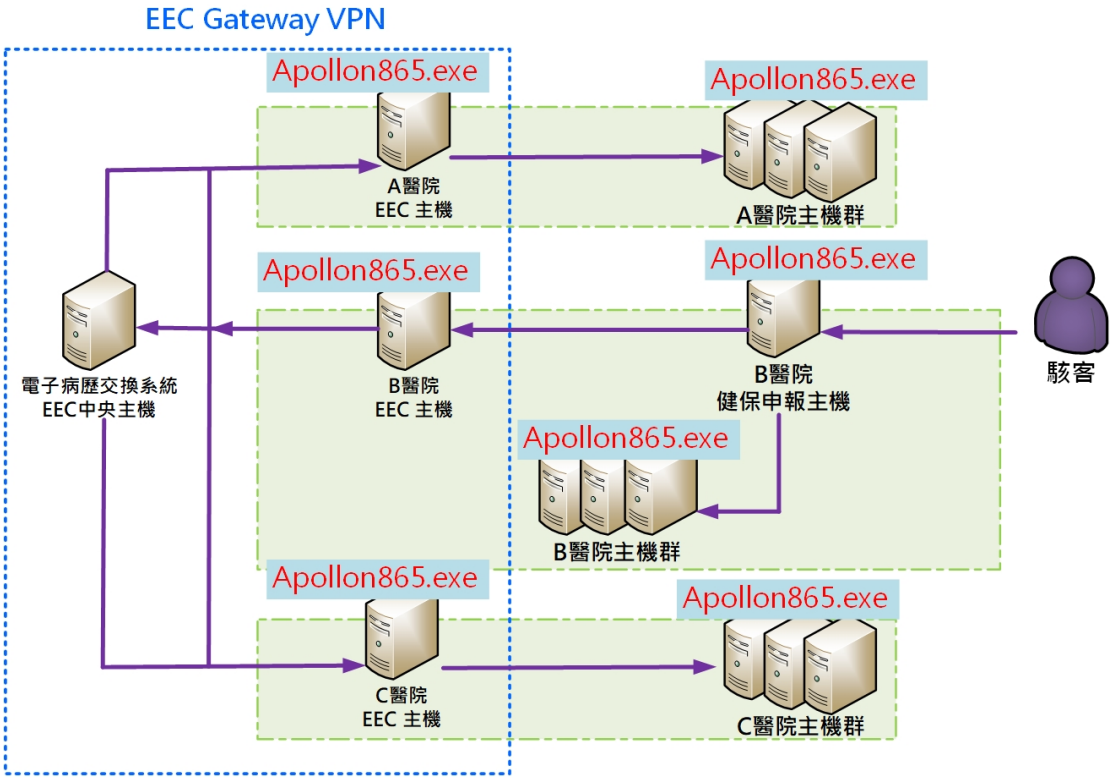
勒索病毒 GlobeImposter
攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 12 月

一、事件簡介

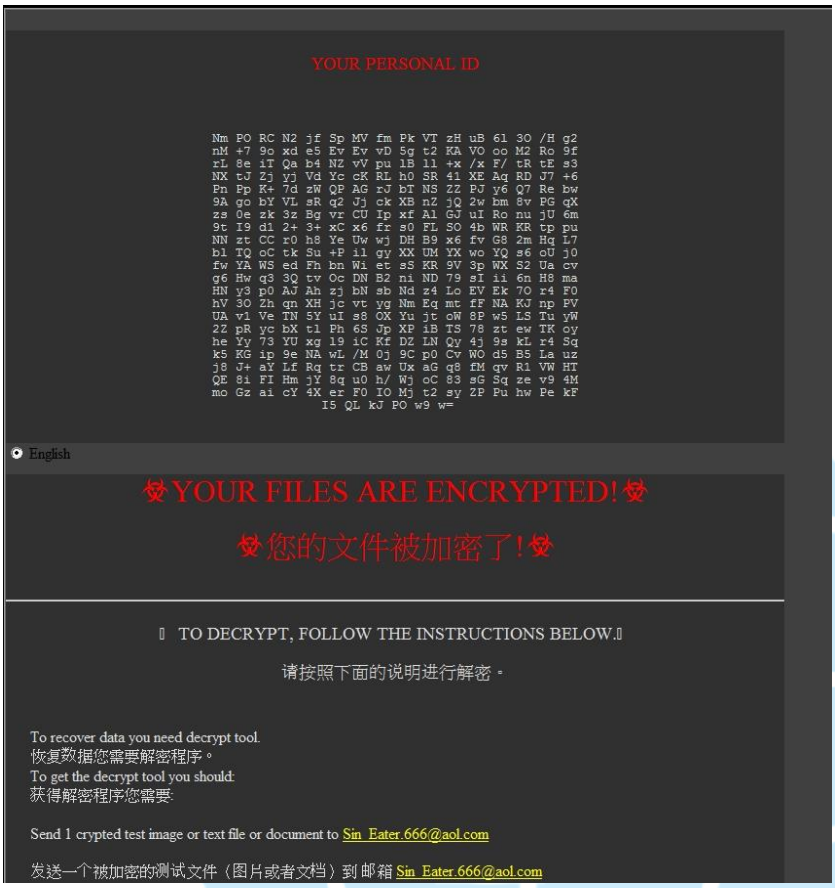
1. 2019/8/29 全台醫療機構陸續傳出電腦主機遭受勒索病毒攻擊，至 2019/9/1 共有 22 家醫院受害。駭客將中毒電腦作為跳板，利用密碼管理與 RDP 漏洞竄入衛福部電子病歷交換系統(EEC)專屬 EEC Gateway VPN 網路，並開始擴散病毒。
2. 由於 EEC 所用 VPN 網路為各大醫院自主管理與共用之內部網路，並未分割 VLAN，造成該勒索病毒得以急速擴散。
3. 本事件爆發之勒索病毒為 GlobeImposter「十二主神」2.0 版本，主要的攻擊程式為 Apollon865.exe，它會通過社交工程或 BlueKeep RDP 漏洞進行擴散，Apollon 中譯為阿波羅，為希臘十二主神之一。



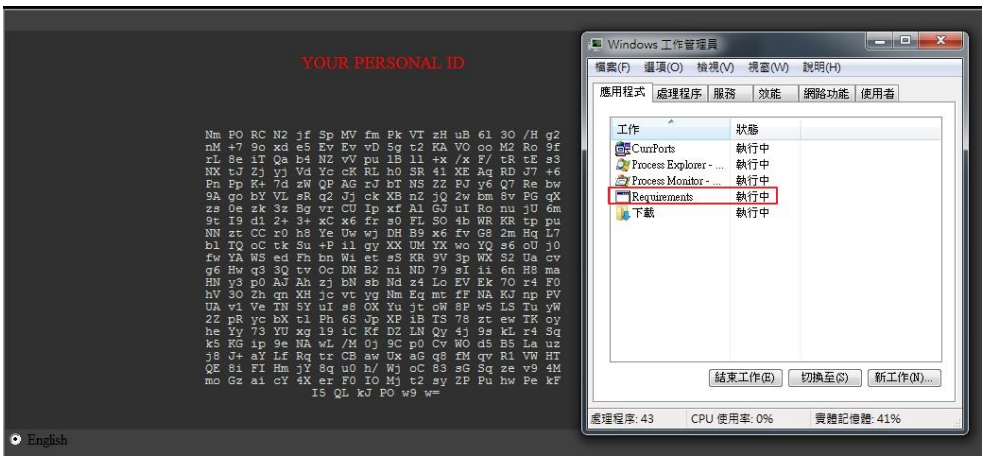
4. 為了解 Apollon865.exe 的攻擊行為與對受害者的危害程度，本中心對病毒樣本進行檢測。

二、事件檢測

1. 首先，使用一台具有網路磁碟與 32 位元 Windows 7 作業系統的虛擬主機，將惡意程式 Apollon865.exe 於該主機上執行，執行後桌面會出現被勒索通知信覆蓋的黑色畫面，無法看到任何可以點選開啟程式或資料夾的路徑。



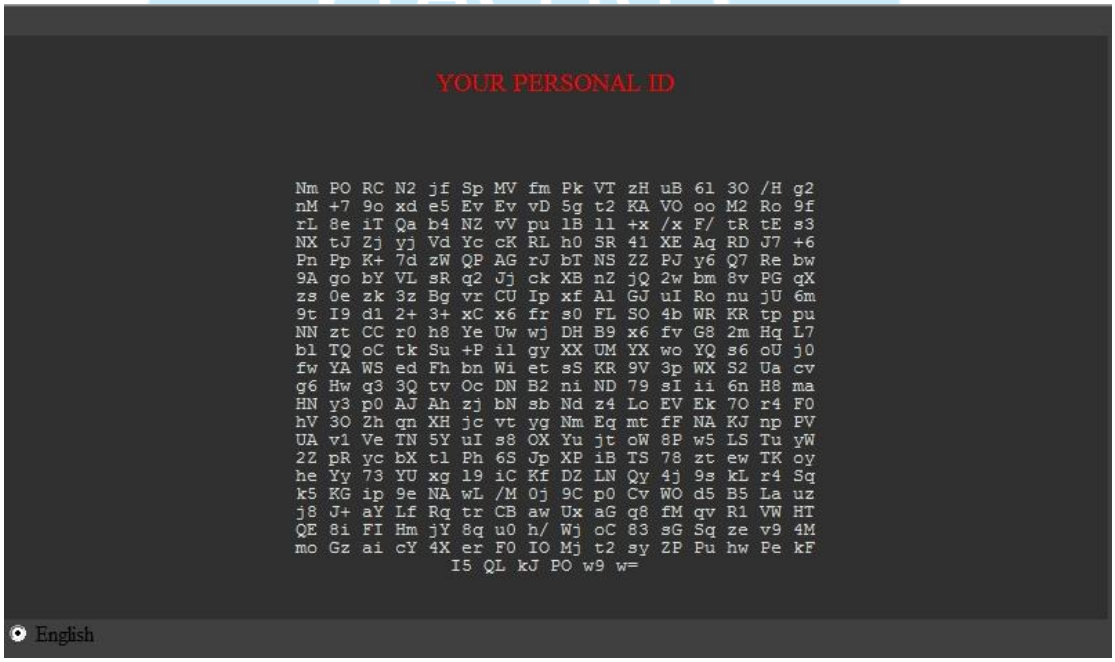
需透過 Ctrl+Alt+Del 開啟「工作管理員」視窗後，結束執行中的 Requirements，才能關閉此勒索通知信的程式，進而出現主機的桌面。



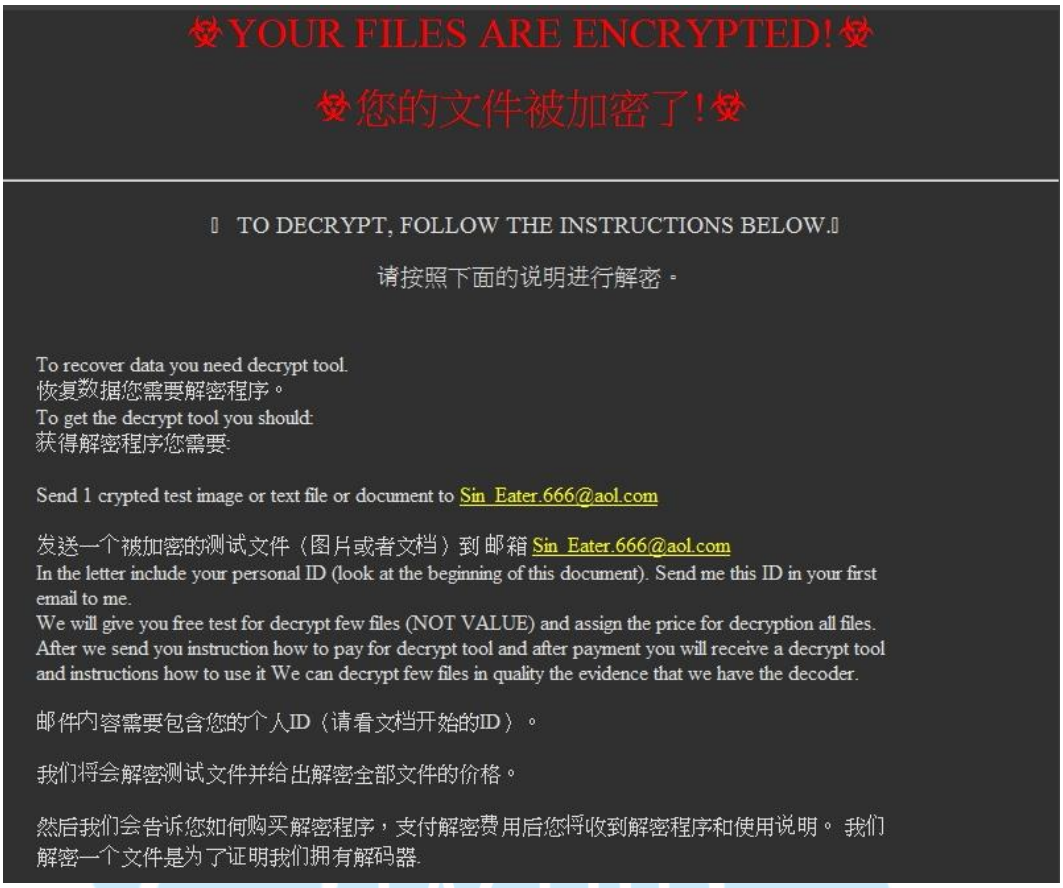
2. 在 Apollon865.exe 執行一段時間後會在原資料夾中消失，只剩下 HOW TO BACK YOUR FILES.exe 與 ids.txt 兩個檔案。

3. 執行 HOW TO BACK YOUR FILES.exe 後，發現其開啟勒索通知信，而以執行檔作為勒索通知信的方式與一般以文字檔當勒索通知信有很大的差別，因為文字檔很容易被關閉，而執行檔的方式若遇無資訊能力的使用者，可能無法將它關閉，容易造成使用者的恐慌。檢視勒索通知信的內容，可分為三個部分:YOUR PERSONAL ID、YOUR FILES ARE ENCRYPTED! 與 MOST IMPORTANT!!!。

(1) YOUR PERSONAL ID:此 ID 提供駭客識別受害者用。

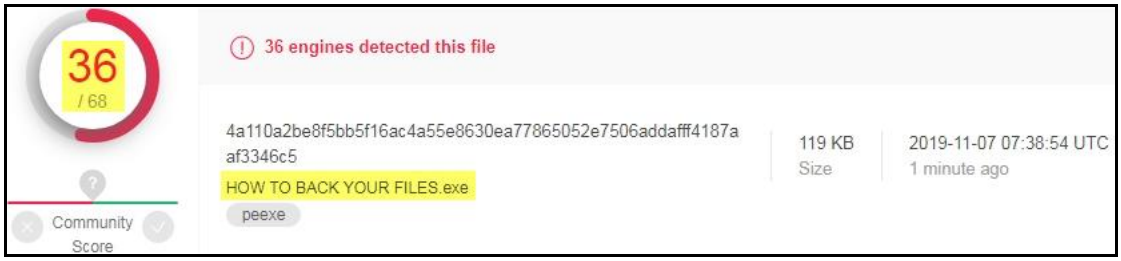


(2) YOUR FILES ARE ENCRYPTED! :告訴受害者電腦內檔案已被加密，如需要解密需寫信至 Sin Eater.666@aol.com，而且信件內容需包含個人 ID，也提到在收到信件後會告訴使用者如何支付解密費用與購買解密器。



(3) MOST IMPORTANT!!! :告訴使用者不要聯繫或相信其他保證能解密文件的人，只有 Sin Eater.666@aol.com 能解密檔案，也提到防毒軟體可能會刪除此勒索通知信。

4. HOW TO BACK YOUR FILES.exe 經 Virustotal 檢測，其惡意比例為 36/68，表示仍有將近一半的防毒軟體無法識別它為惡意檔案。

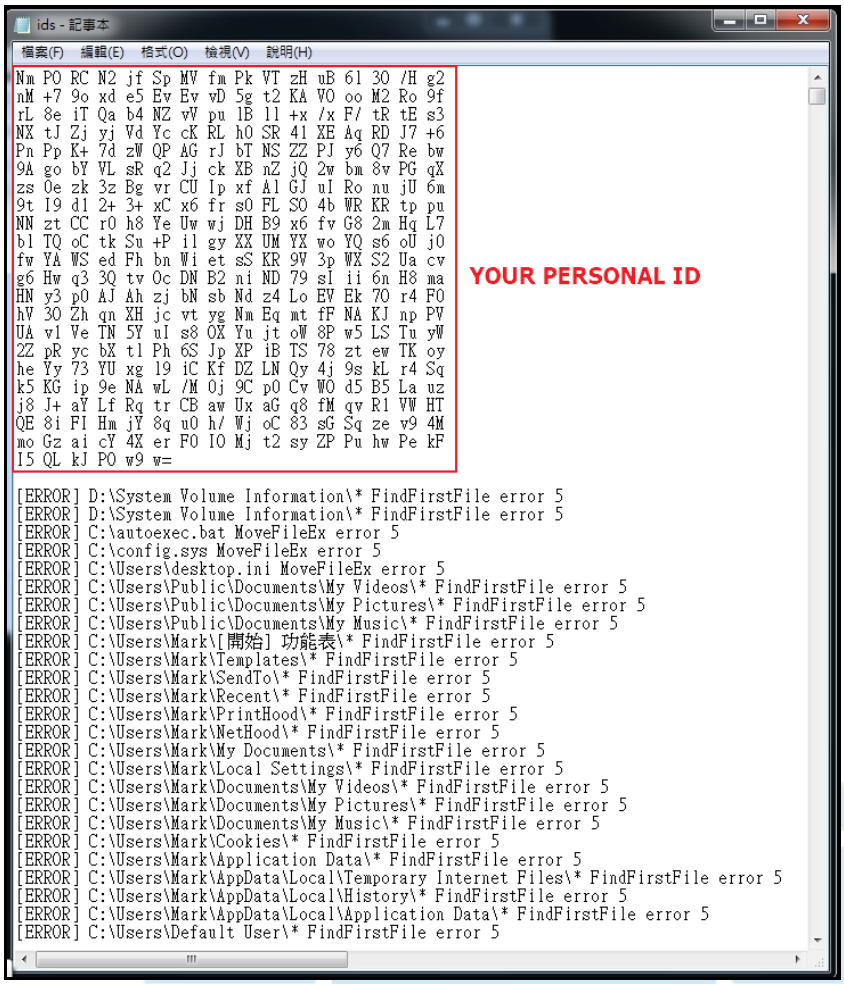


Ad-Aware	Gen:Variant.Johnnie.199748	AhnLab-V3	Trojan/Win32.FileCoder.R291561
ALYac	Gen:Variant.Johnnie.199748	SecureAge APEX	Malicious
Arcabit	Trojan.Johnnie.D30C44	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/FileCoder.yttti
BitDefender	Gen:Variant.Johnnie.199748	BitDefenderTheta	Gen:NN.ZexaF.31988.huW@aSLW5Rji
Cylance	Unsafe	Cyren	W32/Filecoder.S.gen!Eldorado
DrWeb	Trojan.Encoder.29493	eScan	Gen:Variant.Johnnie.199748
ESET-NOD32	Win32/Filecoder.FV	F-Prot	W32/Filecoder.S.gen!Eldorado

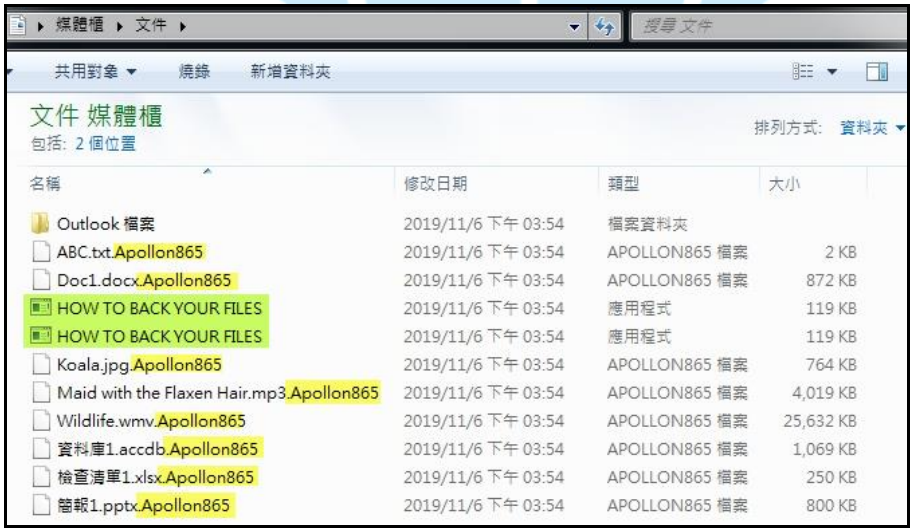
F-Secure	Trojan.TR/FileCoder.yttti	FireEye	Gen:Variant.Johnnie.199748
Fortinet	W32/Generic.AC.44EFB9!tr	GData	Gen:Variant.Johnnie.199748
Ikarus	Trojan-Ransom.FileCrypter	Jiangmin	TrojanDownloader.Generic.bbnb
K7AntiVirus	Trojan (005031101)	K7GW	Trojan (005031101)
Malwarebytes	Ransom.FileCryptor	MAX	Malware (ai Score=85)
Microsoft	Trojan:Win32/Fuerboos.C!cl	NANO-Antivirus	Trojan.Win32.Encoder.fywwmv
Panda	Trj/GdSda.A	Qihoo-360	HEUR/QVM20.1.0FFB.Malware.Gen

Rising	Trojan.Generic@ML.80 (RDMK:Lu0A...	TrendMicro	Ransom.Win32.FAKEGLOBE.SMTH...
TrendMicro-HouseCall	Ransom.Win32.FAKEGLOBE.SMTH...	VBA32	Trojan.Encoder
Yandex	Trojan.Filecoder!sRQJqDg3CHU	Zillya	Trojan.Filecoder.Win32.9903

5. 檢視 ids.txt 內容，發現內容為 YOUR PERSONAL ID 與執行程式時產生錯誤的紀錄，推測該勒索病毒似乎處於調試階段，故病毒加密後會在同目錄下釋放一個 ids.txt，用於存放 ID 和列印錯誤信息。

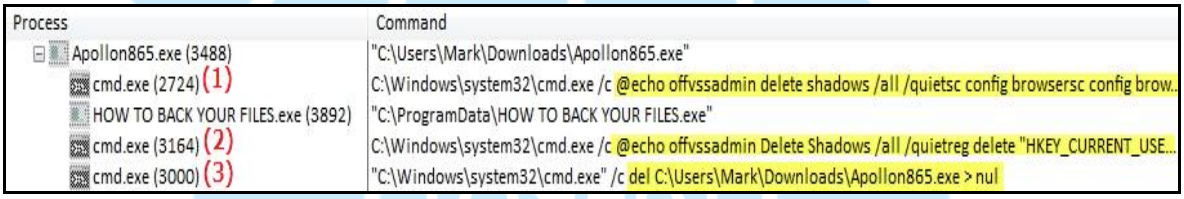


6. 檢視主機內檔案被加密情形，除了 C:\windows 與 C:\Program Files 兩個資料夾內檔案沒有被加密外，主機內的檔案都被加密了。被加密的檔案都會延伸出一個副檔名 Apollon865，而且在每個被勒索病毒拜訪過的資料夾，則會放入勒索通知信 HOW TO BACK YOUR FILES.exe。



查看該主機的網路磁碟機內容，發現裡面的檔案也都被加密了。因此，只要主機有設定網路磁碟機，則裡面的資料一定會感染勒索病毒。

7. 查看背景程式運作情形，發現 Apollon865.exe 執行後會呼叫 3 次 cmd.exe 與 HOW TO BACK YOUR FILES.exe，也會創建勒索通知信「HOW TO BACK YOUR FILES.exe」到各個目錄，而在病毒加密文件後，會複製它到被加密的目錄中。



(1) cmd.exe(2724): 該病毒執行後會先呼叫 cmd.exe(PID:2724)來執行關閉顯示指令、刪除影子副本、啟動瀏覽器與關閉一些資料庫服務。

(2) cmd.exe(3164):在 Apollon865.exe 呼叫 HOW TO BACK YOUR FILES.exe 執行後，會呼叫 cmd.exe(PID:3164)來執行關閉顯示命令、刪除影子副本、變更遠端桌面連線服務機碼的一些設定與刪除所有事件日誌。

```
cmd.exe(3164)
C:\Windows\system32\cmd.exe /c @echo off 關閉顯示命令
vssadmin Delete Shadows /all /quiet 刪除影子副本
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil cl "%1" 刪除所有事件日誌
```

刪除遠端桌面連線服務機碼的預設值
刪除遠端桌面服務機碼的Servers設定值
新增遠端桌面服務機碼的Servers設定值

(3) cmd.exe(3000): Apollon865.exe 執行到最後會呼叫 cmd.exe(PID:3000)，在不讓命令於螢幕上秀出的狀況下來刪除自己本身，這樣使用者也不會察覺到惡意程式所在之處。

```
cmd.exe(3000)
"C:\Windows\system32\cmd.exe" /c del C:\Users\Mark\Downloads\Apollon865.exe > nul
```

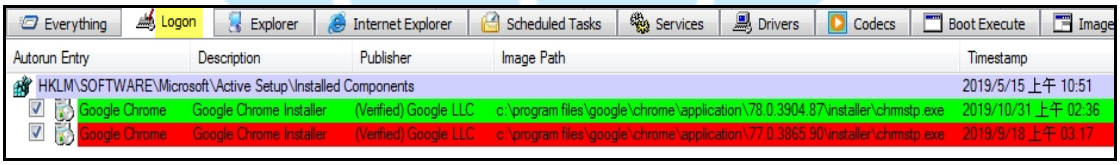
8. 檢視原先主機桌面的 Chrome 連結內容，發現該連結在 Apollon865.exe 執行期間被修改，點擊該連結開啟 Chrome 後，發現 Chrome 呈現軟體安裝過後的初始畫面。

在 C:\使用者\...\AppData\Local\Temp 資料夾內，發現 Chrome 軟體安裝紀錄 chrome_installer.log，而且該檔案修改時間為 Apollon865.exe 執行期間。

在 C:\Program Files\Google\Chrome\Application\78.0.3904.87\Installer 資料夾內發現 Chrome 軟體程式，而且檔案建立日期為 Apollon865.exe 執行期間。

查看主機應用程式安裝與更新狀況，發現該主機在 2019/11/6(Apollon865.exe 執行期間) 有安裝 Google Chrome。

從 AutoRuns 的 Logon 內容得知，Chrome 會在重新開機後自動安裝程式。



Chrome 安裝程式 chrmstp.exe 經 Virustotal 檢測，其惡意比例為 0。

9. 惡意程式 Apollon865.exe(MD5: a37f82d716e96e254a24c45791df752a)經 Virustotal 檢測，其惡意比例為 57/70，非常高，而且有多家防毒軟體公司以

GlobeImposter 命名它。

Ad-Aware	Generic.Ransom.GlobeImposter.FB74...	AegisLab	Trojan.Win32.DelShad.4!c
AhnLab-V3	Malware/Win32.Ransom.C3121937	Alibaba	Trojan:Win32/Maoloa.5bbd7bb4
ALYac	Trojan.Ransom.GlobeImposter	SecureAge APEX	Malicious
Arcabit	Generic.Ransom.GlobeImposter.FB74...	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Maoloa.evrob
BitDefender	Generic.Ransom.GlobeImposter.FB74...	BitDefenderTheta	Gen:Trojan.Heur2.PPBB.3.0.suW@cC...

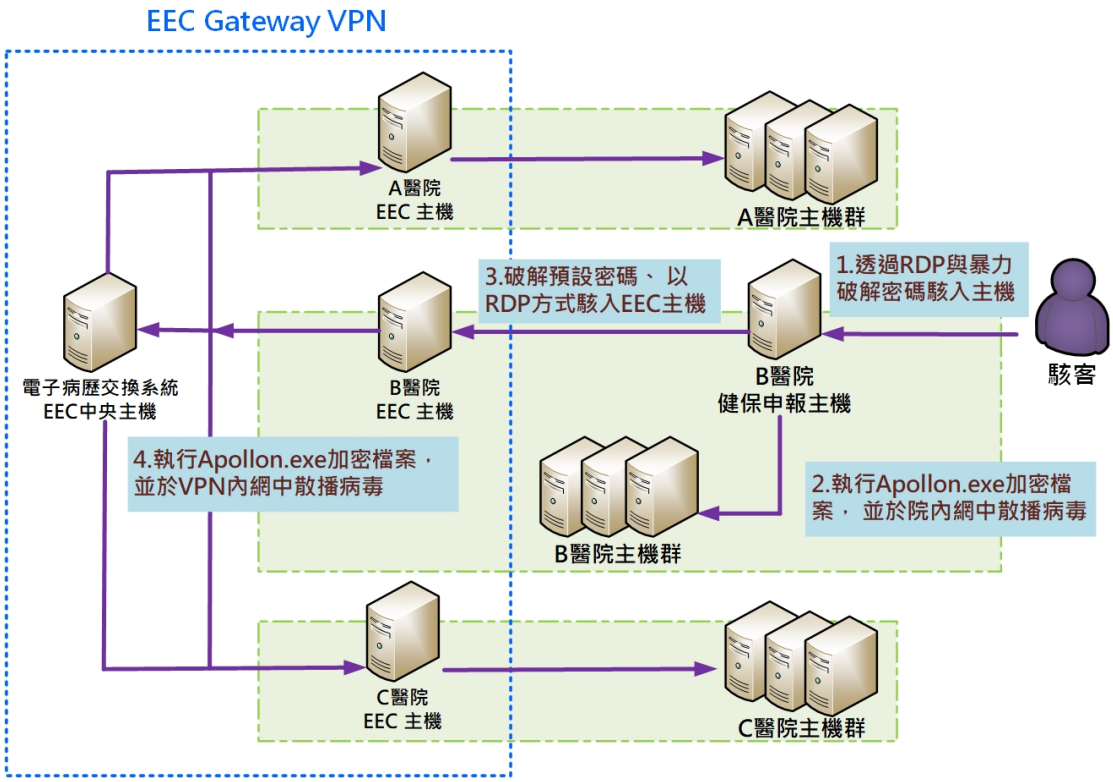
DrWeb	Trojan.Encoder.29413	Emsisoft	Generic.Ransom.GlobeImposter.FB74...
Endgame	Malicious (high Confidence)	eScan	Generic.Ransom.GlobeImposter.FB74...

GData	Generic.Ransom.GlobeImposter.FB74...	Ikarus	Trojan-Ransom.Maoloa

Rising	Ransom.GlobeImposter!1.BC66 (CLA...	SentinelOne (Static ML)	DFI - Suspicious PE
Sophos AV	Troj/Maoloa-A	Sophos ML	Heuristic
Symantec	Downloader	TACHYON	Ransom/W32.GlobeImpostere.304128

10. 將 HOW TO BACK YOUR FILES.exe 與一個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 GlobeImposter 2.0 勒索軟體。

三、事件攻擊行為示意圖



1.駭客透過遠端桌面連線(RDP)與暴力攻擊破解密碼，駭入某醫院健保申報主機。

2.駭客執行勒索軟體 Apollon.exe 來加密檔案，並且於醫院內部網路中散播病毒。

3.駭客破解該醫院所屬 EEC 主機預設密碼，並以 RDP 方式駭入 EEC 主機。

4.駭客執行 Apollon.exe 來加密檔案，並且於 VPN 內網中散播病毒。

四、總結與建議

1. 本事件發生主要因為 RDP 漏洞與密碼被破解造成，駭客以受害主機為跳板，進而攻擊醫院內部網路與 EEC Gateway VPN 網路。
2. 勒索軟體 GlobeImposter 最早被發現是在 2017 年 3 月，在 2018 年該病毒

於中國大陸各醫療機構中流竄，造成不少損失。本事件受害主機所感染的 GlobeImposter 是 2.0 版本，有別於 1.0 版，新增了對於勒索通知信 HOW TO BACK YOUR FILES.exe 的中文敘述。

3. 勒索軟體 GlobeImposter 在執行後會呼叫 cmd.exe 來執行一些指令，它會刪除影子副本、啟動 Browser、關閉一些資料庫服務、刪除所有事件日誌與變更遠端桌面連線服務的設定，最後會刪除自己本身。

4. 將本案的勒索軟體 GlobeImposter 與一般勒索軟體進行特徵比較，整理如下表。

	一般勒索軟體	勒索軟體 GlobeImposter
攻擊(感染)途徑	社交工程(隨機釣魚)	RDP 入侵 EEC VPN 網路
攻擊行為	加密主機內的檔案、刪除影子副本	加密主機內的檔案、關閉顯示指令、刪除影子副本、啟動瀏覽器與關閉一些資料庫服務、變更遠端桌面連線服務機碼的一些設定與刪除所有事件日誌。產生 ids.txt (存放 ID 和列印錯誤信息)
勒索通知信的類型	文字檔	執行檔
執行後是否刪除自身	否	是
勒索對象	一般個人	醫療機構
加密檔案的範圍	除了 C:\windows 與 C:\Program Files 資料夾外的檔案都加密了。	除了 C:\windows 與 C:\Program Files 資料夾外的檔案都加密了。

5. 由該事件可以發現許多現有醫院存在的資安問題，詳述如下。

(1)醫院各主機容易存在弱密碼問題。

(2)醫院對於主機的維護依賴委外廠商居多，容易造成主機管理的遠端連線問題。

(3)醫院對於內部網路的防護措施比外部網路還薄弱。

(4)健保所使用的 EEC gateway VPN 因未切割 VLAN，容易形成所有 EEC 主機都處於同一網路。因此，當一台主機感染病毒，則其他主機也會感染病毒。

6. 針對 GlobeImposter 勒索病毒的攻擊，有下列預防措施提供使用者參考。

(1) 定時更新電腦主機之系統與相關程式，並且修復漏洞。

(2) 對於主機的管理，定期更改帳戶密碼，並設置強密碼，避免使用統一的密碼。

(3) 定期備份重要資料於其他備援裝置中。

(4) 不要隨意開啟或點擊不明來源的郵件(或副檔)。

(5) 不要從不明來源的網站下載軟體或檔案。

(6) 關閉非必要的文件共享權限。

(7) 關閉非必要業務的 RDP 連線。

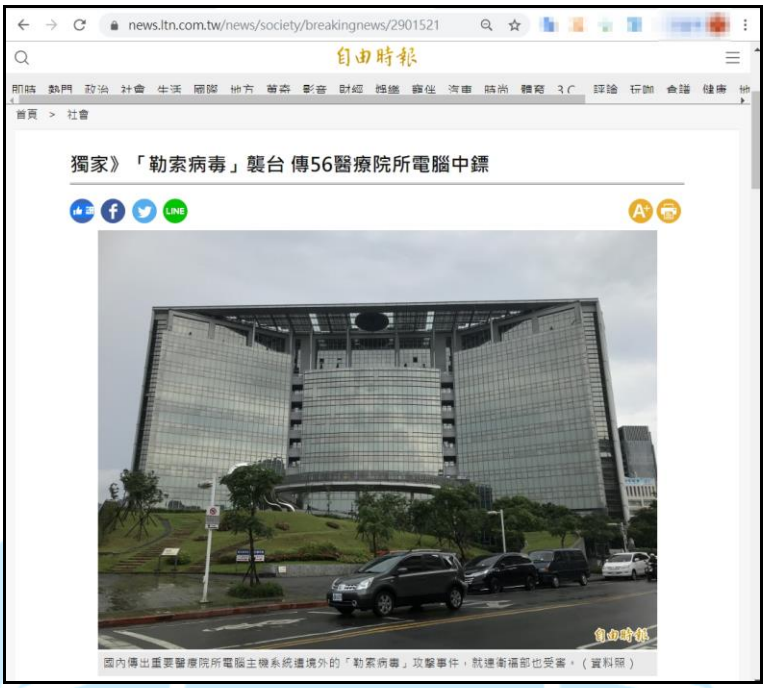
五、相關報導

1.近日 22 家醫療院所遭勒索病毒攻擊事件處理說明

https://dep.mohw.gov.tw/PRO/cp-2732-49147-120.html

2.獨家》「勒索病毒」襲台 傳 56 醫療院所電腦中鏢

https://news.ltn.com.tw/news/society/breakingnews/2901521



3.【徹底揭露 2019 年臺灣最大規模病毒攻擊事件】勒索軟體衝擊！全臺醫療院所資安拉警報

https://www.ithome.com.tw/news/134108