

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

- 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。
- 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。



 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

 首先,使用一台具有網路磁碟與32位元 Windows7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。

YOUR PERSONAL ID	
Nm PO RC N2 jf Sp MV fm Pk VT zH uB 61 30 /H g2 nM +7 90 xd e5 Ev Ev vD Sg t2 NA VO co N2 Rc 93 r1 86 17 ga b4 NC VV pu 1B 11 14 // Ff 45 r6 FN ct 37 ga b4 NC VV pu 1B 11 14 // Ff 45 r6 FN ct 37 ga b4 NC VV pu 1B 11 14 // Ff 45 r6 FN ct 37 ga b4 NC VV pu 1B 11 14 // Ff 45 r6 FN ct 37 f0 VV sA ct 37 NT S 22 2V bm 8 vF 64 X Ph ct 37 f0 VV sA ct 37 NT S 22 2V bm 8 vF 64 X zs 00 EV VV sR q2 jj ck XB n2 10 2v bm 8 vF 64 X zs 00 EV VV sR q2 jj ck XB n2 10 2v bm 8 vF 64 X zs 00 EV VV sR q2 vj ck XB n2 10 2v bm 8 vF 64 X zs 00 EV VV sR q2 vj ck XB n2 10 2v bm 8 vF 64 X zs 00 EV S 2 B9 VC UT px HB 9 x6 fv 68 2m Hq 17 b1 rQ cC tc k Su +P 11 gy XX UM YX wo YQ s6 c0 j0 fw YA WS ed fh bh Wi et sS KR 9 V3 gb XX S2 Ua cv g6 Hw g3 30 tv Oc DN B2 ni ND 79 sI 11 66 HB ma HN y3 DA JA JA j2 NH sB NA z4 Lo EV k7 0 r4 F0 NV 30 2h qn XH jc tv yg Nm Eq mt fF NA K3 np FV UA v1 Ve TN SY UJ 18 60 XF J1 57 R 2z ew TX oy z2 pR yc BX t1 Pi 65 Gp XP 18 15 78 zz ew 17 oy h5 YJA wi 14 LA (KJ DA JA LA (KJ DA SA B4 LA SA Z z5 JA yc BA LA JA 12 LA (JA SA JA SA Z z5 JA yc BA LA JA 12 LA (JA SA JA SA Z z5 JA yc BA LA JA 12 LA (JA SA JA SA Z z5 JA yc BA LA JA 12 LA (JA SA JA SA Z z5 JA yc BA LA JA 12 LA (JA SA JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 12 LA (JA SA Z z5 JA yc BA LA JA 22 JA JA 24 JA 24 JA 25 JA 35 JA 25 JA 35 JA 25 JA	
• English	
♦ YOUR FILES ARE ENCRYPTED! ♦	
★您的文件被加密了!★	
I TO DECRYPT, FOLLOW THE INSTRUCTIONS BELOW.	
· · · · · · · · · · · · · · · · · · ·	
To recover data you need decrypt tool. 恢复数据您需要解密程序。 To get the decrypt tool you should: 获得解密程序您需要:	
Send 1 crypted test image or text file or document to <u>Sin Eater.666@aol.com</u>	
发送,个神的被控制进去处于(图目去关注)和III的答 Sin Tatas 666 @ad ann	

需透過 Ctrl+Alt+Del 開啟「工作管理員」視窗後,結束執行中的 Requirements,

YOUR PERSONAL ID	P Windows工作管理員 場案(P) 導運(P) 検担(A) 提高(M) 説明(H)
Nm FO RC N2 jf Sp MV fm Pk VT zH uB 61 30 /H g2 nM +7 90 xd e5 Ev Ev VD Sg t2 KA VO 30 M2 R0 9f rL 8e 17 Qa b4 N2 VV µ1 B 11 +x /x F/ tR tE 33 NX tJ 2j yj V4 vc KK Lh 05 K4 LK 04 RM DJ7 +6 Pn Fp K+ 7d 2M QP AG JJ o XS m J 10 Q 2W mK VF QG QK 22 06 zX 32 B0 vr CC 10 px f A1 GJ u1 R0 mu JD Gm 91 13 4C 20 3 JA 2X 5 V 10 X 10 X 20 7 R0 b4 17 Q C 2K 30 +P 11 gy XX DM XX 07 82 64 J 17 Q C 2K 30 +P 11 gy XX DM XX 07 86 64 J 17 Q C 7K 80 +P 11 gy XX DM XX 50 66 01 JO fw YA NS e6 4F ho MX is 25 X 11 K0 79 K1 66 H8 m3 HN 35 0A JA 71 JD N8 DK 12 K5 V 10 87 K7 07 4 F0 HN 30 Zh qn XH JC vt y9 Nm Eq mt fF NA KJ np PV UA v1 Ve TN SY U1 S0 CX 10 87 K2 to 87 K3 to 87 JW 22 pR yc bX L1 Ph 65 D7 XP 11 GY 28 zt ew TK 30 pW 22 pR yc bX L1 Ph 65 D7 XP 11 GY 42 yd 38 zt 12 40	應用程式 處理程序 服務 效能 網路功能 使用者 工作 私務 電CurPorts 執行中 Process Monitor - 執行中 Requirements 執行中 下載 執行中
)8 J + AY LF Rq tr CB aw Ux aG q8 fM qv R1 VW HT QE 81 FI Hm JY 8q u0 h/W jo C 83 sG Sq ze v9 HM mo Gz ai CY 44 cF 10 L0 Hj tz sy ZP Pu hw Pe kF IS QL kJ PO w9 w=	【結束工作(E) 【 切換至(S) 】 新工作(N)
● English	產還程序:43 CPU使用率:0% 費體記得體:41%

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。

🚺 🕨 Mark 🕨 下載			▼ \$
▼ 加入至媒體櫃 ▼ 共用對象	き▼ 燒錄 新増資活	料夾	
名稱 ^	修改日期	類型	大小
HOW TO BACK YOUR FILES	2019/11/6 下午 03:54	應用程式	119 KB
📄 ids	2019/11/6 下午 03:54	文字文件	808 KB

- 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。

	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	AV fm Pk VT zH uB 61 30 /H VV vD 5g VZ KA VO oo M2 Ro VV pu 1B 11 +x /x F/ tR tE KR LhO SR 41 XE Aq RD J7 G rJ bT NS ZZ PJ yq Q7 Re J ck XB nZ jQ 2w bm 8v PG J ck XB nZ jQ 2w bm 8v PG U Ip xf Al GJ uI Ro nu JU t6 fr 30 FL SO 4b WR KR tp Ww J DH B9 x6 fv G8 2m Hq 1 gy XX UM YX wo YQ s6 0U N B2 ni ND 79 sI ii 6n H8 NN sb Nd z4 Lo EV Ek 70 r4 ty gNm Eq mt fF NA KJ np t8 OX Yu jt oW 8P w5 LS Tu S Jp XP 1B TS 78 zt ew TK (C Kf DZ LN Qy 4J 9s kL r4 M 0j 9C p0 Cv WO d5 B5 La B aw Ux aG g8 fM qv R1 VW NO h/W j0 C 83 3G Sq ze v9 NO IO Mj t2 sy ZP Pu hw Pe , kJ PO w9 w=	g2 9f s3 +6 bw qX 6m pu L7 J0 cv ma F0 cv yW oy yW oy Sq uz HT 4M kF
 English 			

(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。

	services that promise to decrypt your files, this is fraud on their part! They will buy a ad you will pay more for his services. No one, except <u>Sin Eater.666@aol.com</u> will decrypt your files.
• Only <u>Sin Eater.</u>	<u>666@aol.com</u> can decrypt your files
Only <u>Sin Eater.</u> Do not trust any	<u>.666@aol.com</u> can decrypt your files yone besides <u>Sin Eater.666@aol.com</u>
 Only <u>Sin Eater.</u> Do not trust any Antivirus progra Attempts to self 	<u>.666@aol.com</u> can decrypt your files rone besides <u>Sin_Eater.666@aol.com</u> ams can delete this document and you can not contact us later. E-decrypting files will result in the loss of your data
 Only <u>Sin Eater</u>. Do not trust any Antivirus progra Attempts to self Decoders other 	<u>666@aol.com</u> can decrypt your files yone besides <u>Sin_Eater.666@aol.com</u> ams can delete this document and you can not contact us later. F-decrypting files will result in the loss of your data users are not compatible with your data, because each user's unique encryption key
 Only <u>Sin Eater</u>. Do not trust any Antivirus progra Attempts to self Decoders other 只有 <u>Sin Eater</u> 	<u>666@aol.com</u> can decrypt your files yone besides <u>Sin Eater.666@aol.com</u> ms can delete this document and you can not contact us later. -decrypting files will result in the loss of your data users are not compatible with your data, because each user's unique encryption key <u>.666@aol.com</u> 能解密您的文件。
 Only <u>Sin Eater</u>. Do not trust any Antivirus progra Attempts to self Decoders other 只有 <u>Sin Eater</u> (只有 Cate) 	<u>666@aol.com</u> can decrypt your files yone besides <u>Sin Eater.666@aol.com</u> mus can delete this document and you can not contact us later. E-decrypting files will result in the loss of your data users are not compatible with your data, because each user's unique encryption key <u>666@aol.com</u> 能解密您的文件。 人,除了 <u>500</u> matrix como
 Only <u>Sin Eater</u>. Do not trust any Antivirus progra Attempts to self Decoders other 只有 <u>Sin Eater</u> 不要相信任何 杀黄软件会册 	<u>666@aol.com</u> can decrypt your files yone besides <u>Sin Eater.666@aol.com</u> ams can delete this document and you can not contact us later. F-decrypting files will result in the loss of your data users are not compatible with your data, because each user's unique encryption key <u>.666@aol.com</u> 能解密您的文件。 人,除了 <u>Sin Eater.666@aol.com</u> 。 除这个文档,那么您将无法联系到我们。
 Only <u>Sin Eater</u> Do not trust any Antivirus progra Attempts to self Decoders other 只有 <u>Sin Eater</u> 不要相信任何 杀毒软件会删 尝试自己去解 	<u>6666@aol.com</u> can decrypt your files yone besides <u>Sin Eater.666@aol.com</u> ams can delete this document and you can not contact us later. E-decrypting files will result in the loss of your data users are not compatible with your data, because each user's unique encryption key <u>666@aol.com</u> 能解密您的文件。 人,除了 <u>Sin Eater.666@aol.com</u> 。 除这个文档,那么您将无法联系到我们。 密文件将会使您的数据丢失。

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。

36	① 36 engines detected this file			
Community Score	4a110a2be8f5bb5f16ac4a55e8630ea77865052e7506addafff4187a af3346c5 HOW TO BACK YOUR FILES,exe peexe		119 KB 2019-11-07 07:38:54 UT Size 1 minute ago	
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	1 Trojan.TR/FileCoder.yttti	FireEye	() Gen:Variant.Johnnie.199748	
Fortinet	U W32/Generic.AC.44EFB9ltr	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.Clcl	NANO-Antivirus	① Trojan.Win32.Encoder.fywwmv	
Panda	() Trj/GdSda.A	Qihoo-360	() HEUR/QVM20.1.0FFB.Malware.Gen	
Rising	① 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	① 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。



📕 ids - 記事本	
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)	
$\begin{array}{llllllllllllllllllllllllllllllllllll$	YOUR PERSONAL ID
<pre>[ERROR] D:\System Volume Information* FindFirst [ERROR] D:\System Volume Information* FindFirst [ERROR] D:\System Volume Information* FindFirst [ERROR] C:\autoexec.bat MoveFileEx error 5 [ERROR] C:\Users\desktop.ini MoveFileEx error 5 [ERROR] C:\Users\Public\Documents\My Videos* Fi [ERROR] C:\Users\Public\Documents\My Music* Find [ERROR] C:\Users\Public\Documents\My Music* Find [ERROR] C:\Users\Mark\Cemplates* FindFirstFile [ERROR] C:\Users\Mark\SendTo* FindFirstFile err [ERROR] C:\Users\Mark\SendTo* FindFirstFile err [ERROR] C:\Users\Mark\SendTo* FindFirstFile err [ERROR] C:\Users\Mark\NetHood* FindFirstFile [ERROR] C:\Users\Mark\NetHood* FindFirstFile [ERROR] C:\Users\Mark\Documents\My Videos* Find [ERROR] C:\Users\Mark\Documents\My Videos* FindFirst [ERROR] C:\Users\Mark\Documents\My Videos* FindFirst [ERROR] C:\Users\Mark\Documents\My Music* FindFirstFile er [ERROR] C:\Users\Mark\Documents\My M</pre>	File error 5 File error 5 FindFirstFile error 5 FindFirstFile error 5 File error 5 For 5 For 5 For 5 File error 5 File error 5 File error 5 File error 5 FirstFile error 5 FirstFile error 5 Strot 5 FirstFile error 5 Strot 5 Trot 5 FirstFile error 5 Trot 5 Trot 5 Trot 5 Trot 5 FirstFile error 5 Trot 5

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。

▶ 媒體櫃 ▶ 文件 ▶	*	4 搜导文件	
• 共用對象 ▼ 燒錄 新増資料夾) = • =
文件 媒體櫃 包括: 2 個位置			排列方式: 資料夾 🔻
名稱 ^	修改日期	類型	大小
]] Outlook 檔案	2019/11/6 下午 03:54	檔案資料夾	
ABC.txt.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	2 KB
Doc1.docx.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	872 KB
HOW TO BACK YOUR FILES	2019/11/6 下午 03:54	應用程式	119 KB
HOW TO BACK YOUR FILES	2019/11/6 下午 03:54	應用程式	119 KB
Koala.jpg.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	764 KB
Maid with the Flaxen Hair.mp3.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	4,019 KB
Wildlife.wmv.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	25,632 KB
□ 資料庫1.accdb.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	1,069 KB
☐ 檢查清單1.xlsx.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	250 KB
☐ 簡報1.pptx <mark>.Apollon865</mark>	2019/11/6 下午 03:54	APOLLON865 檔案	800 KB

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。

🚽 🕨 電腦 🕨 File Doc (\\DAVID-PC) (Z:)	▼ 49	搜尋 File Doc (
▼ 燒錄 新增資料夾			
名稱	修改日期	類型	大小
Excel1.xlsx.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	10 KB
HOW TO BACK YOUR FILES	2019/11/6下午 03:54	應用程式	119 KB
NETWORK.pptx.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	34 KB
You.txt.Apollon865	2019/11/6下午 03:54	APOLLON865 檔案	1 KB
📄 哈喔.docx. <mark>Apollon865</mark>	2019/11/6 下午 03:54	APOLLON865 檔案	13 KB
□ 資料庫1.accdb.Apollon865	2019/11/6 下午 03:54	APOLLON865 檔案	433 KB

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。

Process	Command
🖃 🌆 Apollon865.exe (3488)	"C:\Users\Mark\Downloads\Apollon865.exe"
cmd.exe (2724) (1)	C:\Windows\system32\cmd.exe /c @echo offvssadmin delete shadows /all /quietsc config browsersc config brow.
HOW TO BACK YOUR FILES.exe (3892)	"C:\ProgramData\HOW TO BACK YOUR FILES.exe"
📖 cmd.exe (3164) (2)	C:\Windows\system32\cmd.exe /c @echo offvssadmin Delete Shadows /all /quietreg delete "HKEY_CURRENT_USE
cmd.exe (3000) (3)	"C:\Windows\system32\cmd.exe" /c del C:\Users\Mark\Downloads\Apollon865.exe > nul

(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。

cmd.exe(2724)
C:\Windows\system32\cmd.exe /c @echo off 關閉顯示指令
vssadmin delete shadows /all /quiet 刪除影子副本
sc config browser
sc config browser start=enabled
sc stop vss 關門 vcc
sc config vss start=disabled
sc stop MongoDB
sc config MongoDB start=disabled 關闭MongoDB
sc stop SQLWriter 開閉日 COL Minitor
sc config SQLWriter start=disabled
sc stop MSSQLServerOLAPService
sc config MSSQLServerOLAPService start=disabled 關闭 MSSQLServerOLAPService
sc stop MSSQLSERVER
sc config MSSQLSERVER start=disabled 關闭MSSQLSERVER
sc stop MSSQL\$SQLEXPRESS 器時期SSQL \$SQL EXPRESS
sc config MSSQL\$SQLEXPRESS start=disabled
sc stop ReportServer
sc config ReportServer start=disabled
sc stop OracleServiceORCL 图即OracleServiceORCL
sc config OracleServiceORCL start=disabled
sc stop OracleDBConsoleorcl 關間OracleDBConsoleorcl
sc config OracleDBConsoleorcl start=disabled
sc stop OracleMTSRecoveryService
sc config OracleMTSRecoveryService start=disabled 關闭OracleMTSRecoveryService
sc stop OracleVssWriterORCL 图即OracleVcsWriterOPCL
sc config OracleVssWriterORCL start=disabled
sc stop MySQL
sc config MySQL start=disabled 開闭可以与QL

(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。



(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。

👩 Google Chr	ome - 內容		
一般捷徑	相容性 安全性 詳細資料 以前的版本	● EDER Overe × + ← → C ● Chrome drains://welcome	× 0 1
	Google Chrome		
檔案類型:	捷徑 (.lnk)		
描述:	Google Chrome	只要簡單幾個步驟就能完成瀏覽器設定	
位置:	C:\Users\Public\Desktop	打造專屬的 Chrome	
大小:	2.05 KB (2,105 位元組)		
磁碟大小:	4.00 KB (4,096 位元組)	開始使用 已经是 Chrome 使用者了嗎? 請見人感戶	
建立日期:	2019年5月15日,上午10:51:00		
修改日期:	2019年11月6日,下午 03:53:26		
存取日期:	2019年5月15日,上午 10:51:00		

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。

🗼 🕨 電腦 🕨 本機磁	碟 (C:)) Program Files	► Google ► Chrome	 Application 	n 🖡 78.0.3904.87	7 🕨 Installer
◆ 加入至媒體櫃 ◆	• 共用對象 ▼ 燒	錄 新增資料夾			
名稱	修改日期	建立日期	類型	大小	
Chrmstp.exe	2019/11/6 下午 03:52	2019/11/6下午 03:53	應用程式	1,882 KB	
chrome.7z	2019/11/6下午 03:52	2019/11/6下午03:52	7Z 檔案	208,468 KB	
🐻 setup.exe	2019/11/6 下午 03:52	2019/11/6下午 03:53	應用程式	1,882 KB	

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。

	集 🕨 程式和功能				◆ 投尋程式和功能
控制台首頁 檢視安裝的更新 發 開啟或關閉 Windows 功能	解除安裝或變更程式 若要解除安裝程式,請從清單選取程式,然後按一下[解除安裝]、[變更]或[修復]。 組合管理 ▼				
	名稱	發行者	安裝於	大小	版本
	Google Chrome	Google LLC	2019/11/6		78.0.3904.87
	Microsoft Office	Microsoft Corporation	2019/10/4		15.0.4420.1017

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

🖅 Everything 🛛 🎪 Logon	Explorer 🥭	Internet Explorer	Scheduled Tasks	🆏 Services	Drivers	Codecs	Boot Execute	📑 Image
Autorun Entry	Description	Publisher	Image Path				Timestamp	
HKLM\SOFTWARE\Micros	oft\Active Setup\Installed C	omponents					2019/5/15	午 10:51
🔽 💮 Google Chrome 🛛	Google Chrome Installer	(Verified) Google LLC	c:\program files\goog	le\chrome\applica	ition\78.0.3904.8	7\installer\chmstp	.exe 2019/10/31_	上午 02:36
🗹 🚺 Google Chrome 🛛	Google Chrome Installer	(Verified) Google LLC	c:\program files\goog	le\chrome\applica	ition \77.0.3865.9	0\installer\chmstp	.exe 2019/9/18	:午 03:17

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

	⊘ No engines detected this file		
	fa4f52457f4d9e3a5eb2b1a2294432f4639865524039cb7640fd6f9 497d2c7ad setup.exe	1.84 MB Size	2019-11-06 08:38:03 UTC a moment ago
Community	detect-debug-environment overlay peexe runtime-modules	signed	

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。

57	① 57 engines detected this file		
Community	bdc09fbf3df995437454a60067af617551ccdd 69b5ce Apollon865.txt peexe	cbbd77eda2bcd03280a2	297 KB 2019-11-06 07:49:56 UTC Size a moment ago
Ad-Aware	() Generic.Ransom, Globelmposter, FB74	AegisLab	() Trojan.Win32.DelShad.4lc
AhnLab-V3	() Malware/Win32.Ransom.C3121937	Alibaba	① Trojan:Win32/Maoloa.5bbd7bb4
ALYac	① Trojan.Ransom <mark>.Globelmposter</mark>	SecureAge APEX	① Malicious
Arcabit	() Generic.Ransom, Globelmposter, FB74	Avast	() Win32:Malware-gen
AVG	() Win32:Malware-gen	Avira (no cloud)	() TR/Maoloa.evrob
BitDefender	() Generic.Ransom.Globelmposter.FB74	BitDefenderTheta	() Gen:Trojan.Heur2.PPBB.3.0.suW@cC
DrWeb	① Trojan.Encoder.29413	Emsisoft	① Generic.Ransom <mark>.GlobeImposter.</mark> FB74
Endgame	 Malicious (high Confidence) 	eScan	① Generic Ransom Globelmposter FB74
GData	() Generic.Ransom <mark>.GlobeImposter.</mark> FB74	Ikarus	 Trojan-Ransom.Maoloa
Rising	() Ransom. <mark>Globelmposter</mark> I1.BC66 (CLA	SentinelOne (Static ML)	① DFI - Suspicious PE
Sophos AV	() Troj/Maoloa-A	Sophos ML	() Heuristic
Symantec	() Downloader	TACHYON	① Ransom/W32.Globelmpostere.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。

GlobeImposter 2.0
This ransomware has no known way of decrypting data at this time.
It is recommended to backup your encrypted files, and hope for a solution in the future.
Identified by

sample_extension: .Apollon865

Click here for more information about GlobeImposter 2.0
Would you like to be notified if there is any development regarding this ransomware? Click here.

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

- 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	
	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	
攻擊行為	TA CEDT	些資料庫服務、變更遠端	
大手打小		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	
	除了 C:\windows 與	除了 C:\windows 與	
加密檔案的範圍	C:\Program Files 資料	C:\Program Files 資料夾	
	夾外的檔案都加密了。	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

