勒索病毒 GoGaLocker 攻擊

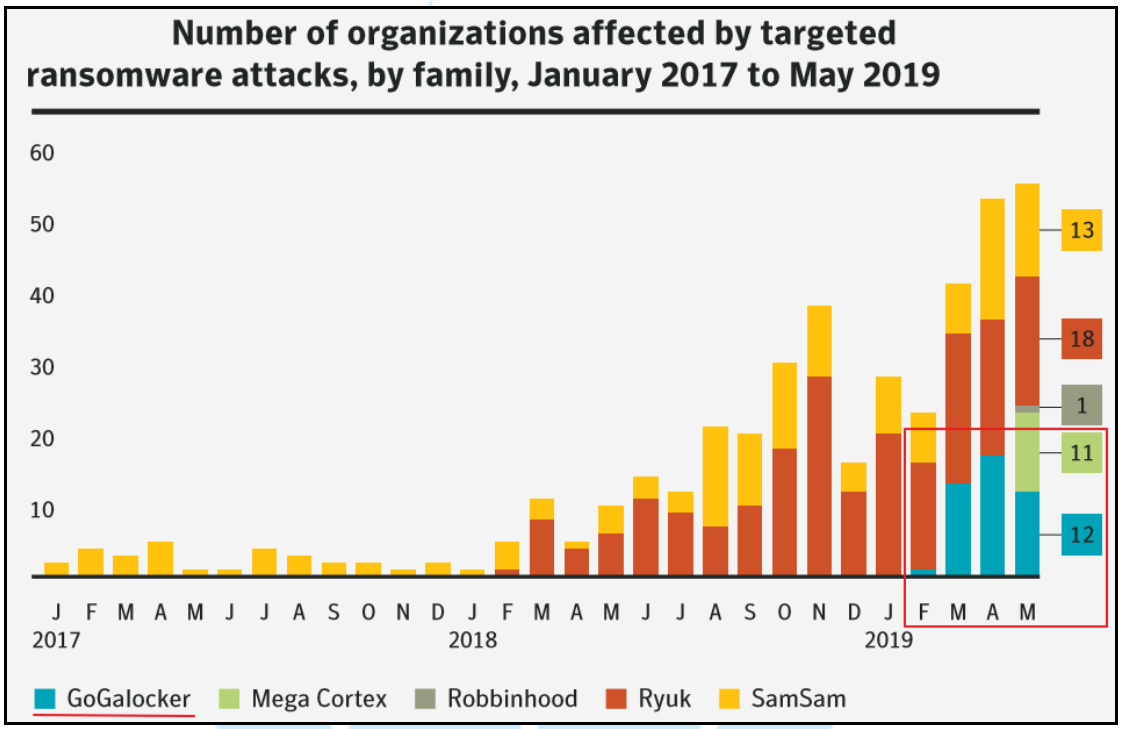
事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 9 月

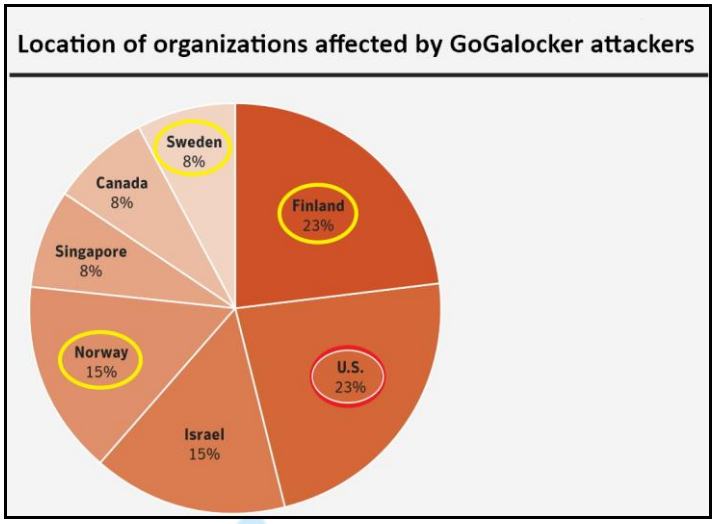
一、事件簡介

1. 知名資安公司賽門鐵克在2019年7月所發佈的「TARGETED RANSOMWARE: An ISTR Special Report」報告指出，GoGalocker是2019年1月出現的一種新的目標式勒索軟體威脅，而從2017年1月至2019年5月受目標式勒索軟體家族攻擊影響的組織數量圖可以看到，GoGalocker在2019年2月開始有攻擊行為。



(資料來源:賽門鐵克 TARGETED RANSOMWARE: An ISTR Special Report)

2. 自從2019年初首次出現以來，GoGalocker已經攻擊了各行業領域的組織，包括電腦服務、會計和審計、諮詢、金融服務、電動工具、建築和施工、金融服務、出版、印刷、金屬和倉儲等。這些目標組織中有23%位於美國，但除此之外，斯堪的納維亞(Scandinavia)的受害者比例很高，包括芬蘭（23%），挪威（15%）和瑞典（8%）。



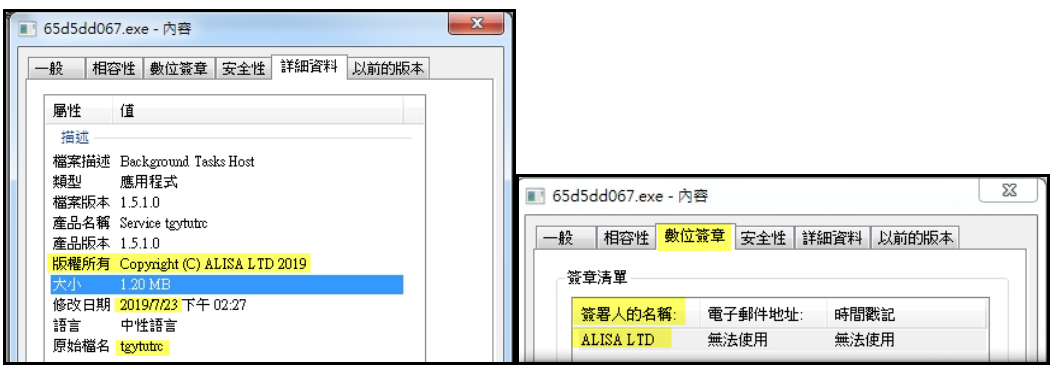
(資料來源:賽門鐵克 TARGETED RANSOMWARE: An ISTR Special Report)

3. 為了解 GoGaLocker 之攻擊行為與危害程度，本中心取得樣本後進行檢測。

二、事件檢測

1. 首先，使用一台有 Windows 7 32 位元作業系統的虛擬主機，並且將 GoGaLocker 樣本 65d5dd067.exe (MD5: 438ebec995ad8e05a0cea2e409bfd488) 放於該主機內。

2. 在執行前檢視 65d5dd067.exe 的內容，發現該程式的數位簽章是由 ALISA LTD 所簽署，推測此為駭客用合法的憑證對其勒索軟體進行數位簽章的隱藏手法，藉此避免惡意程式被發現。



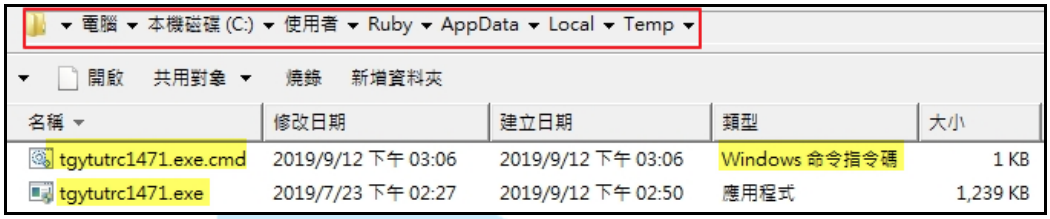
3. 65d5dd067.exe 經 Virustotal 檢測，其惡意比例為 59/68，而且有多家防毒軟體公司以 Lockergoga 命名它。

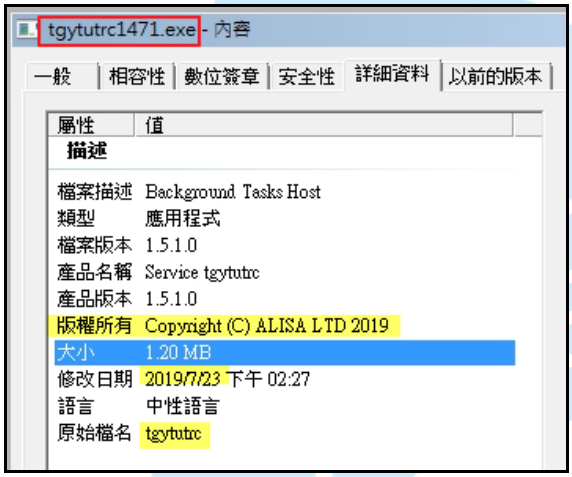
Ad-Aware	Trojan.Ransom.LockerGoga.C	AegisLab	Trojan.Win32.Crypren.4!c
AhnLab-V3	Win-Trojan/Alisa.Exp	Alibaba	Ransom:Win32/LockerGoga.190327
ALYac	Trojan.Ransom.Filecoder	Antiy-AVL	Trojan[Ransom]/Win32.Crypren
SecureAge APEX	Malicious	Arcabit	Trojan.Ransom.LockerGoga.C
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]

Avira (no cloud)	TR/AD.LockerGaga.tugmc	BitDefender	Trojan.Ransom.LockerGoga.C
CAT-QuickHeal	Trojan.Multi	ClamAV	Win.Ransomware.Lockergoga-6918486-0
Comodo	Malware@#2jbclhsb71r17	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.995ad8	Cylance	Unsafe
Cyren	W32/LockerGoga.B.gen!Eldorado	DrWeb	Trojan.MulDrop9.5759
eGambit	PE.Heur.InvalidSig	Emsisoft	MalCert.A (A)
Endgame	Malicious (high Confidence)	eScan	Trojan.Ransom.LockerGoga.C
ESET-NOD32	A Variant Of Win32/Filecoder.LockerGog...	F-Prot	W32/LockerGoga.B.gen!Eldorado
F-Secure	Trojan.TR/AD.LockerGaga.tugmc	FireEye	Trojan.Ransom.LockerGoga.C
Fortinet	W32/LockerGoga.Dltr.ransom	GData	Trojan.Ransom.LockerGoga.C
Ikarus	Trojan-Ransom.LockerGoga	Jiangmin	Trojan.Crypren.ob

K7AntiVirus	Trojan (00549a691)	K7GW	Trojan (00549a691)
Kaspersky	Trojan-Ransom.Win32.Crypren.afft	Malwarebytes	Backdoor.Remcos
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.7164915.susgen
McAfee	Ransom-Goga!438EBEC995AD	McAfee-GW-Edition	Ransom-Goga!438EBEC995AD
Microsoft	Ransom:Win32/LockerGoga	NANO-Antivirus	Trojan.Win32.Encoder.fohkpc
Palo Alto Networks	Generic.ml	Panda	Trj/Ransomcrypt.M
Qihoo-360	Win32/Trojan.826	Rising	Ransom.LockerGoga!1.B635 (CLASSIC)
SentinelOne (Static ML)	DFI - Suspicious PE	Sophos AV	Troj/Ransom-FHW
Sophos ML	Heuristic	Symantec	Downloader
TACHYON	Ransom/W32.LockerGoga.1268602	Tencent	Win32.Trojan.Crypren.Pbzi
VBA32	TrojanRansom.Crypren	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.S.LockerGoga.1268602	Webroot	W32.Ransom.Lockergoga
Yandex	Trojan.Cryprenly2pJ56Epl9M	Zillya	Trojan.Crypren.Win32.881
ZoneAlarm by Check Point	Trojan-Ransom.Win32.Crypren.afft	Lastline	MALWARE RANSOM
NSFOCUS POMA	TROJAN	Acronis	Undetected

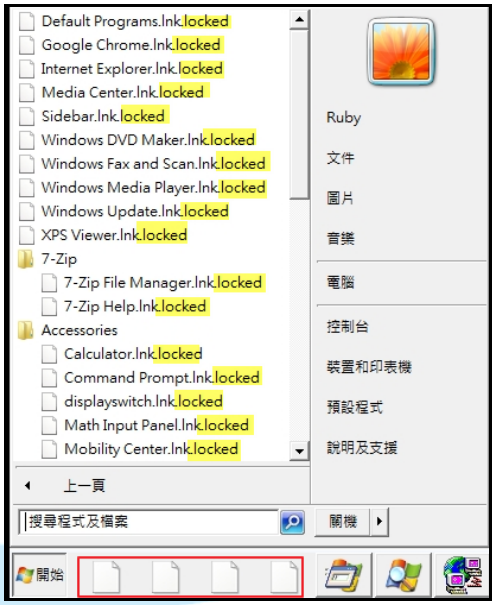
4. 執行 65d5dd067.exe 後，發現該程式在其所在之位置原地消失，但在 C:\使用者\Ruby\AppData\Local\Temp 資料夾內會發現另一個與它相同的程式 tgytutrc[4 位亂數].exe(如 tgytutrc1471.exe)，而且在 Temp 資料夾內也會產生一個 tgytutrc[4 位亂數].exe.cmd(如 tgytutrc1471.exe.cmd)的 Windows 命令指令碼。

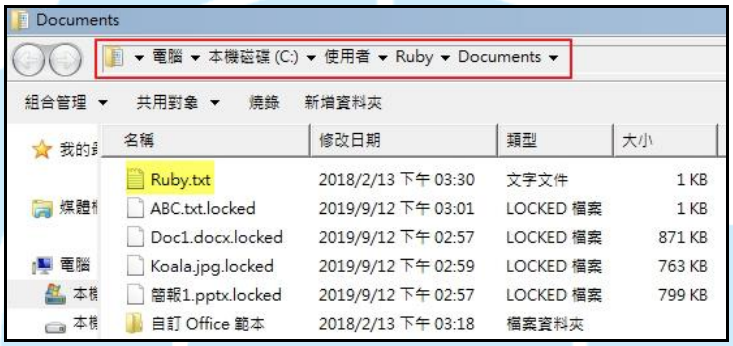




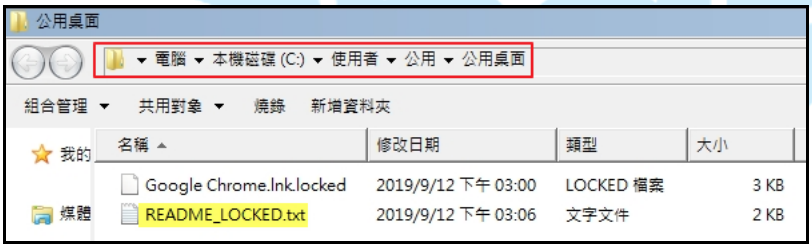
查看 tgytutrc1471.exe.cmd 內容，發現 3 行指令，第一行指令是 timeout 3，之後第二行與第三行指令是刪除 tgytutrc1471.exe 與 tgytutrc1471.exe.cmd。

5. 在執行 65d5dd067.exe 後，主機陸續出現檔案被加密的狀態，而且被加密的檔案皆會延伸出一個.locked 的副檔名。除了將檔案加密外，該程式也會將視窗設定的背景顏色全部改為淺灰色，而在桌面左下角的工作列圖示也變成白色。在加密後查看主機檔案被加密情形，發現除了 C:\windows 資料夾內的檔案與 txt 文字檔沒被加密外，主機內的檔案都被加密。

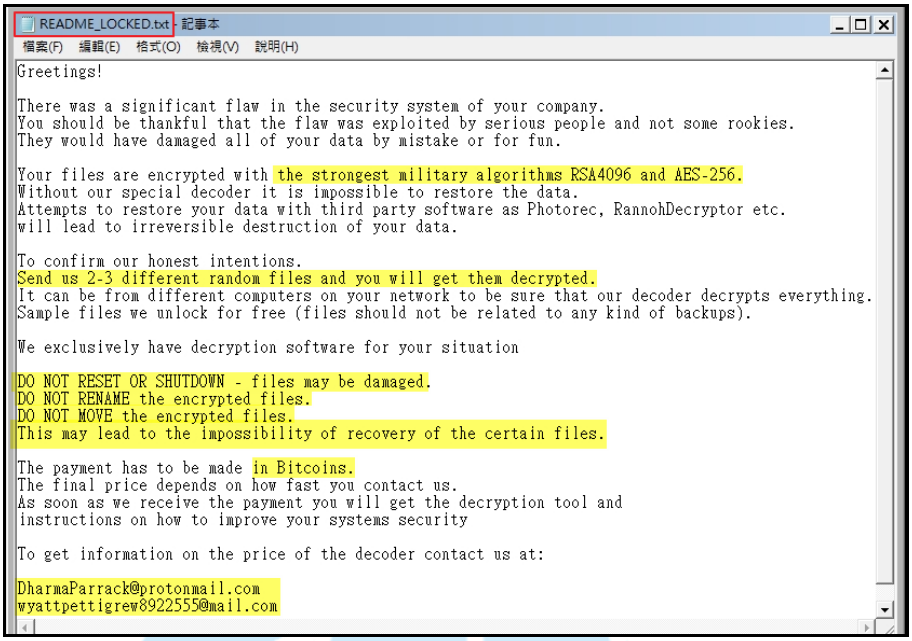




6. 65d5dd067.exe 對主機內檔案進行加密後，在主機公用桌面會出現一個 README_LOCKED.txt 的勒索通知信。



從該文字檔內容得知，加密是使用最強的軍事演算法 RSA4096 與 AES-256，受害者可以寄 2-3 個不同的檔案給駭客進行解密，並且建議受害者不要隨意重新開機或關機、不要對已被加密的檔案更改檔案名稱、不要移動已被加密的檔案，因為這些行為可能導致檔案無法復原。最後駭客告訴受害者以比特幣支付贖金，並且需寫信至 DharmaParrack@protonmail.com 或 wyattpettigrew8922555@mail.com 來取得贖金金額的資訊。



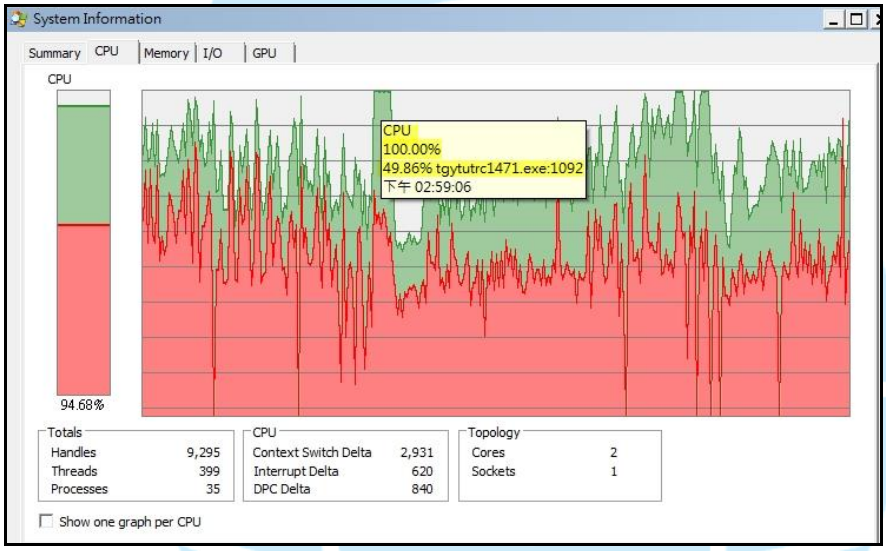
7. 檢視背景程式運作情形，從 Command 可以得知 65d5dd067.exe 執行後會將自己移動到 C:\Users\Ruby\AppData\Local\Temp 資料夾內，並且更名為 tgytutrc1471.exe，之後 tgytutrc1471.exe(PID:1092)會呼叫 logoff.exe、net.exe 與執行多次的 tgytutrc1471.exe，其中 logoff.exe 為工作階段登出公用程式，net.exe 會呼叫 net1.exe 來更改具有系統管理者權限的使用者之密碼，推測更改後的密碼為「HuHuHUHoHo283283@dJD」，而之後執行多次的 tgytutrc1471.exe 來開始加密主機內各檔案。

Process	Command
65d5dd067.exe (2696)	"C:\Users\Ruby\Downloads\65d5dd067.exe"
65d5dd067.exe (1124)	"C:\Users\Ruby\Downloads\65d5dd067.exe"
cmd.exe (2364)	C:\Windows\system32\cmd.exe /c move /y C:\Users\Ruby\Downloads\65d5dd067.exe C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe
tgytutrc1471.exe (1092)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -m
logoff.exe (2164)	C:\Windows\system32\logoff.exe 0
logoff.exe (1952)	C:\Windows\system32\logoff.exe 0
logoff.exe (2000)	C:\Windows\system32\logoff.exe 0
logoff.exe (924)	C:\Windows\system32\logoff.exe 0
logoff.exe (1048)	C:\Windows\system32\logoff.exe 0
net.exe (2236)	C:\Windows\system32\net.exe user Administrator HuHuHUHoHo283283@dJD
net1.exe (2452)	C:\Windows\system32\net1 user Administrator HuHuHUHoHo283283@dJD
net.exe (3352)	C:\Windows\system32\net.exe user Ming HuHuHUHoHo283283@dJD
net1.exe (588)	C:\Windows\system32\net1 user Ming HuHuHUHoHo283283@dJD
net.exe (3480)	C:\Windows\system32\net.exe user Ruby HuHuHUHoHo283283@dJD
net1.exe (2384)	C:\Windows\system32\net1 user Ruby HuHuHUHoHo283283@dJD
tgytutrc1471.exe (3024)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -i SM-tgytutrc -s
tgytutrc1471.exe (1188)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -i SM-tgytutrc -s
tgytutrc1471.exe (1684)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -i SM-tgytutrc -s
tgytutrc1471.exe (3528)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -i SM-tgytutrc -s

在加密檔案完成後會呼叫 cipher.exe 來清理 C 與 D 兩磁碟區，以解除配置的空間。之後會執行 netsh.exe 將區域連線停用、停用介面 Loopback Pseudo-Interface 1 與介面 isatap。接著會執行 tgytutrc1471.exe.cmd 的命令來暫停命令處理 3 秒鐘，之後執行 logff.exe 來成功登出系統。

Process	Command
tgytutrc1471.exe (3384)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -i SM-tgytutrc -s
tgytutrc1471.exe (1708)	C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe -i SM-tgytutrc -s
cipher.exe (2804)	C:\Windows\system32\cipher.exe /w: C:\
cipher.exe (2976)	C:\Windows\system32\cipher.exe /w: D:\
netsh.exe (3836)	C:\Windows\system32\netsh.exe interface set interface 區域連線 DISABLED
netsh.exe (2076)	C:\Windows\system32\netsh.exe interface set interface "Loopback Pseudo-Interface 1" DISABLED
netsh.exe (1328)	C:\Windows\system32\netsh.exe interface set interface isatap.{9CCBC919-5657-48FE-92F2-65E41FB51C1C} DISABLED
cmd.exe (3592)	cmd /c C:\Users\Ruby\AppData\Local\Temp\tgytutrc1471.exe.cmd
timeout.exe (3500)	timeout 3
logoff.exe (2672)	C:\Windows\system32\logoff.exe 0
logoff.exe (4028)	C:\Windows\system32\logoff.exe 1
logoff.exe (4040)	C:\Windows\system32\logoff.exe 1
logoff.exe (3400)	C:\Windows\system32\logoff.exe 0
logoff.exe (3588)	C:\Windows\system32\logoff.exe 0
logoff.exe (1988)	C:\Windows\system32\logoff.exe 0
logoff.exe (2768)	C:\Windows\system32\logoff.exe 0

8. 檢視主機系統效能，發現 CPU 使用率將近 100%，而且有 49%的使用率被 tgytutrc1471.exe 所使用，可見該程式在加密檔案的過程會佔用許多 CPU 的資源。



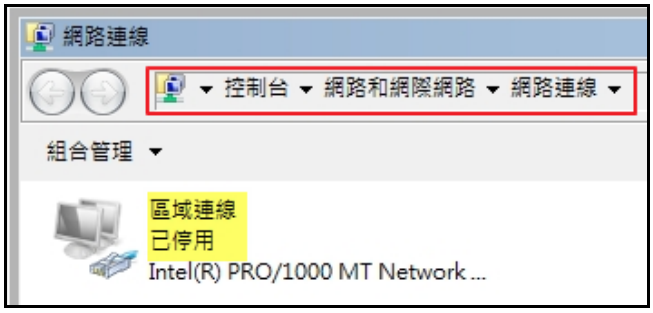
tgytutrc1471.exe	49.45	2,728 K	6,916 K	1092 Background Tasks Host	ALISA LTD
tgytutrc1471.exe		1,956 K	6,352 K	3112 Background Tasks Host	ALISA LTD
tgytutrc1471.exe		1,520 K	5,924 K	972 Background Tasks Host	ALISA LTD
tgytutrc1471.exe	2.84	1,752 K	5,472 K	3864 Background Tasks Host	ALISA LTD
tgytutrc1471.exe	2.95	1,760 K	5,504 K	4020 Background Tasks Host	ALISA LTD

9. 在程式 65d5dd067.exe 執行一段時間後，主機會自動進行使用者登出作業，登出後發現使用者圖示變成空白，而且無法使用原來的密碼登入，同時在主機上的其他使用者也出現無法使用原密碼登入的情形。從背景程式 net.exe 的運作，猜測密碼可能為「HuHuHUHoHo283283@dJD」，以此密碼嘗試登入，結果發現只有擁有系統管理者權限的使用者可用此密碼成功登入系統，一般使用者會出現無法載入使用者設定檔的訊息。

查看 Net.exe 的 command 內容，發現該程式更改 Administrator、Ming、Ruby 等三個擁有系統管理者權限的使用者之密碼，而一般使用者 Maya 雖然密碼沒被更改，但是因使用者設定檔無法載入，故無法登入，推測可能使用者設定檔已遺失，而以帳戶 Ruby 登入系統，發現在 C:\使用者資料夾內找不到使用者 Maya 所屬資料夾。

net.exe (2236)	C:\Windows\system32\net.exe user Administrator HuHuHUHoHo283283@dJD
net1.exe (2452)	C:\Windows\system32\net1 user Administrator HuHuHUHoHo283283@dJD
net.exe (3352)	C:\Windows\system32\net.exe user Ming HuHuHUHoHo283283@dJD
net1.exe (588)	C:\Windows\system32\net1 user Ming HuHuHUHoHo283283@dJD
net.exe (3480)	C:\Windows\system32\net.exe user Ruby HuHuHUHoHo283283@dJD
net1.exe (2384)	C:\Windows\system32\net1 user Ruby HuHuHUHoHo283283@dJD

在以「帳戶 Ruby、密碼:HuHuHUHoHo283283@dJD」成功登入系統後，會發現該主機的網卡是停用狀態，無法連上網路，需重新啟用網卡後才可上網。



10. 查看 65d5dd067.exe 的程式原始碼，發現該程式會特別針對下列副檔名的檔案進行加密:

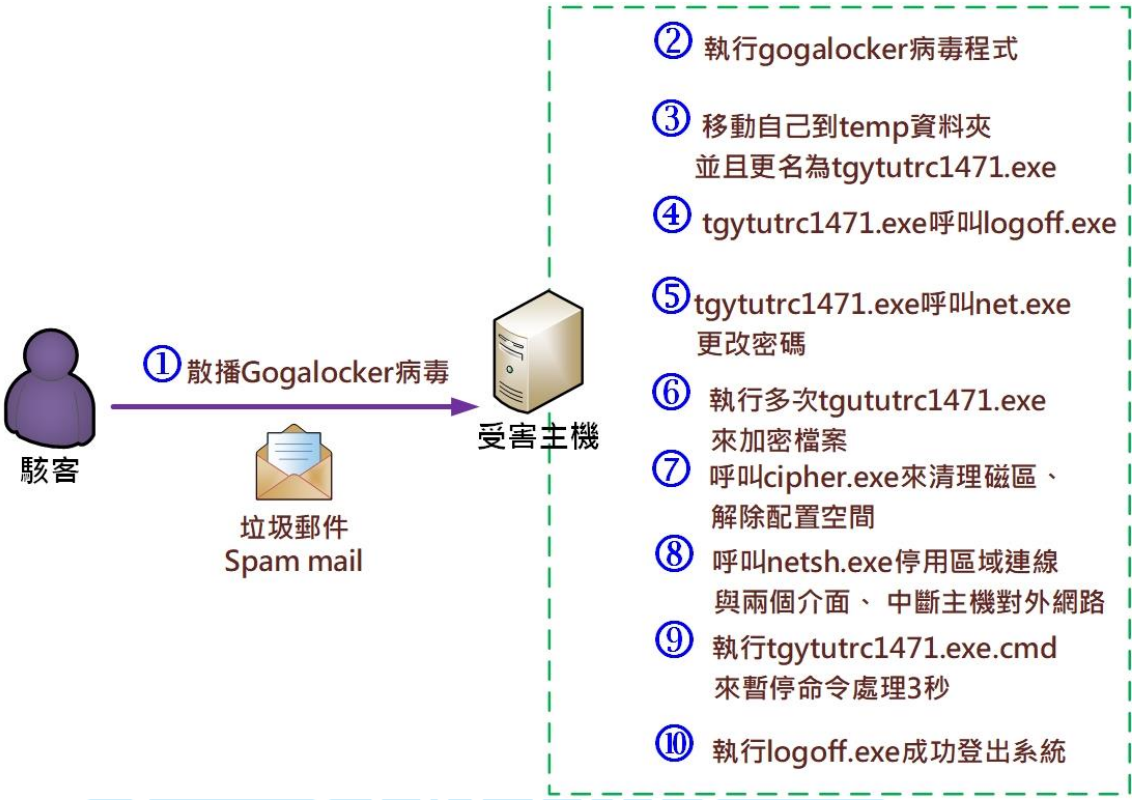
「.link、.doc、.doc、.docx、.docb、.dotx、.dotb、.wkb、.xml、.xls、.xlsx、.xlt、.xltx、.xlsb、.xlw、.ppt、.pps、.pot、.ppsx、.pptx、.posx、.potx、.sldx、.pdf、.db、.sql、.cs、.ts、.js、.py」

```
.rdata:00500AFC                 unicode 0, < \([xX]86\)>,0
.rdata:00500B14 a_lnk           db '.lnk',0             ; DATA XREF: .text:0040CBE8↑o
.rdata:00500B19                 align 4
.rdata:00500B1C a_doc           db '.doc',0             ; DATA XREF: .text:0040BF4E↑o
.rdata:00500B21                 align 4
.rdata:00500B24 a_dot           db '.dot',0             ; DATA XREF: .text:0040BF7F↑o
.rdata:00500B29                 align 4
.rdata:00500B2C a_docx          db '.docx',0            ; DATA XREF: .text:0040BFB0↑o
.rdata:00500B32                 align 4
.rdata:00500B34 a_docb          db '.docb',0            ; DATA XREF: .text:0040BFE1↑o
.rdata:00500B3A                 align 4
.rdata:00500B3C a_dotx          db '.dotx',0            ; DATA XREF: .text:0040C012↑o
.rdata:00500B42                 align 4
.rdata:00500B44 aDotb           db 'dotb',0             ; DATA XREF: .text:0040C043↑o
.rdata:00500B49                 align 4
.rdata:00500B4C a_wkb           db '.wkb',0             ; DATA XREF: .text:0040C074↑o
.rdata:00500B51                 align 4
.rdata:00500B54 a_xml           db '.xml',0             ; DATA XREF: .text:0040C0A5↑o
.rdata:00500B59                 align 4
.rdata:00500B5C a_xls           db '.xls',0             ; DATA XREF: .text:0040C0EB↑o
.rdata:00500B61                 align 4
.rdata:00500B64 a_xlsx          db '.xlsx',0            ; DATA XREF: .text:0040C107↑o
.rdata:00500B6A                 align 4
.rdata:00500B6C a_xlt           db '.xlt',0             ; DATA XREF: .text:0040C138↑o
.rdata:00500B71                 align 4
.rdata:00500B74 a_xltx          db '.xltx',0            ; DATA XREF: .text:0040C169↑o
```

```
.rdata:00500B7C a_xlsb          db '.xlsb',0            ; DATA XREF: .text:0040C19A↑o
.rdata:00500B82                 align 4
.rdata:00500B84 a_xlw           db '.xlw',0             ; DATA XREF: .text:0040C1CB↑o
.rdata:00500B89                 align 4
.rdata:00500B8C a_ppt           db '.ppt',0             ; DATA XREF: .text:0040C1FC↑o
.rdata:00500B91                 align 4
.rdata:00500B94 a_pps           db '.pps',0             ; DATA XREF: .text:0040C22D↑o
.rdata:00500B99                 align 4
.rdata:00500B9C a_pot           db '.pot',0             ; DATA XREF: .text:0040C25E↑o
.rdata:00500BA1                 align 4
.rdata:00500BA4 a_ppsx          db '.ppsx',0            ; DATA XREF: .text:0040C2A4↑o
.rdata:00500BAA                 align 4
.rdata:00500BAC a_pptx          db '.pptx',0            ; DATA XREF: .text:0040C2C0↑o
.rdata:00500BB2                 align 4
.rdata:00500BB4 a_posx          db '.posx',0            ; DATA XREF: .text:0040C2F1↑o
.rdata:00500BBA                 align 4
.rdata:00500BBC a_potx          db '.potx',0            ; DATA XREF: .text:0040C322↑o
.rdata:00500BC2                 align 4
.rdata:00500BC4 a_sldx          db '.sldx',0            ; DATA XREF: .text:0040C353↑o
.rdata:00500BCA                 align 4
.rdata:00500BCC a_pdf           db '.pdf',0             ; DATA XREF: .text:0040C384↑o
.rdata:00500BD1                 align 4
.rdata:00500BD4 a_db            db '.db',0              ; DATA XREF: .text:0040C3B5↑o
.rdata:00500BD8 a_sql           db '.sql',0             ; DATA XREF: .text:0040C3E6↑o
```

```
.rdata:00500BDD                 align 10h
.rdata:00500BE0 a_cs            db '.cs',0              ; DATA XREF: .text:0040C417↑o
.rdata:00500BE4 a_ts            db '.ts',0              ; DATA XREF: .text:0040C45D↑o
.rdata:00500BE8 a_js            db '.js',0              ; DATA XREF: .text:0040C479↑o
.rdata:00500BEC a_py            db '.py',0              ; DATA XREF: .text:0040C4AA↑o
```

三、事件攻擊行為示意圖



1.駭客利用垃圾郵件附件或其他方式散播 Gogalocker 病毒。

2.使用者在受害主機上執行 gogalocker 病毒程式。

3.gogalocker 程式移動自己到 temp 資料夾，並且更名為 tgytutrc1471.exe。

4.tgytutrc1471.exe 呼叫 logoff.exe。

5.tgytutrc1471.exe 呼叫 net.exe 來更改有系統管理者權限之使用者的密碼。

6.執行多次 tgytutrc1471.exe 來加密受害主機內的檔案。

7.呼叫 cipher.exe 清理磁區與解除配置的空間。

8.呼叫 netsh.exe 停用區域網路與兩個介面，使主機無法對外連網。

9.執行 tgytutrc1471.exe.cmd 來暫停命令處理 3 秒鐘。

10.執行 logoff.exe 成功登出系統。

四、總結與建議

1. 勒索病毒 Gogalocker 在執行後會在原地消失，並且在使用者的隱藏資料夾 AppData\local\Temp 內出現，一般使用者無法輕易地發現它的存在，此手法類似無檔案式的勒索病毒。
2. Gogalocker 病毒使用 ALISA LTD 所簽署的數位簽章來偽裝自己是一個合法的程式，藉此規避防毒軟體的偵測。
3. 除了 C:\windows 內的檔案與 txt 文字檔外，該病毒會將主機內的檔案都加密，並且將主機的視窗背景顏色變更為淺灰色。
4. 它與以往的勒索病毒不同，它會更改具有系統管理者權限的使用者之密碼，而且該病毒執行一段時間後會登出系統，導致受害者無法登入系統。
5. Gogalocker 病毒在加密作業完成、登出系統之前，會停用主機的網卡，關閉主機的區域網路連線功能，讓主機完全無法連網。
6. 受害者因為密碼被更改而無法登入系統，將導致無法查看勒索通知信的內容，推測使用者與駭客取得聯繫的機會很低，也可得知此病毒對受害主機的破壞程度很大，推測駭客的主要目的可能不是勒索金錢。
7. 針對 Gogalocker 病毒的攻擊，有下列預防措施提供使用者參考。
   (1) 不隨意下載或執行不明來源的程式。
   (2) 中斷非必要的網路磁碟機連線。如必要連線，可設定檔案為 Read-only 唯讀。
   (3) 停用 AutoPlay 功能，以防止自動執行可執行的檔案。
   (4) 關閉並刪除主機內不必要的服務，以減少可能被攻擊的路徑。
   (5) 設定電子郵件伺服器來阻止或刪除包含常用於傳播病毒的附件檔案的電子郵件，例如.vbs，.bat，.exe，.pif 和.scr 等附件檔案。
   (6) 定期進行系統更新與病毒碼更新，並且定期進行主機的掃毒作業。
   (7) 定期備份主機內的資料。

五、相關資料

1. 賽門鐵克「TARGETED RANSOMWARE: An ISTR Special Report」報告 (2019 年 7 月)

http://images.mktgassets.symantec.com/Web/Symantec/%7Bb464dc43-2ae0-4912-8758-b153d8f278e7%7D_Targeted_Ransomware_2019July.pdf

2. Targeted Ransomware: Proliferating Menace Threatens Organizations

https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat