TLP :WHITE

新勒索病毒 Leakthemall 變種.genesis 病毒分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

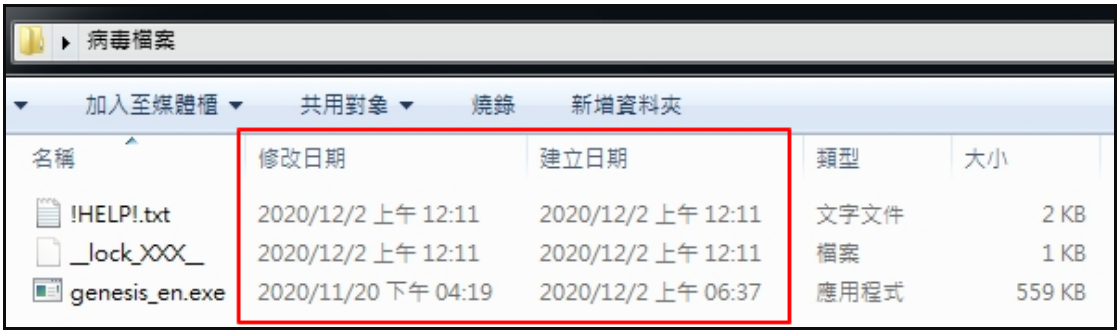
2020 年 12 月

一、事件簡介

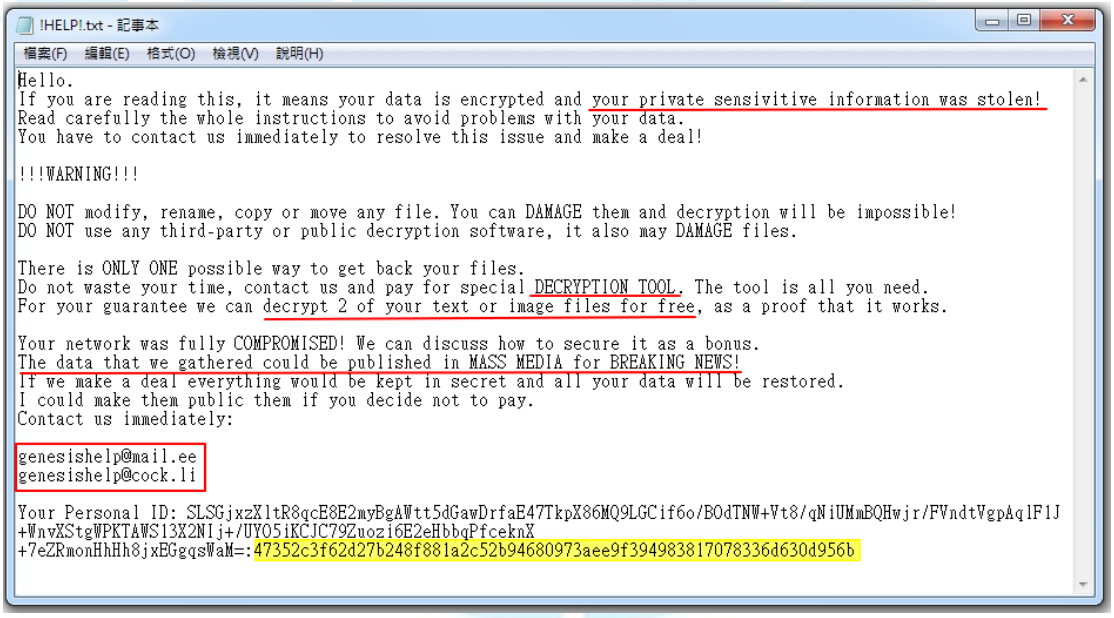
1. 自 2020/09 中旬有多間學校 NAS 感染勒索病毒 AgeLocker 後，在 2020/10/24 發生一所高中有四台 NAS 感染勒索病毒 Phobos 的事件。之後，在 2020/12/02 又發生 Y 高中存放行政業務文件的 NAS 內文件被加密之事件。
2. 從 Y 高中的 DHCP Server 發現有駭客入侵後建立一個帳號並且連線 NAS 的足跡，而該 DHCP Server 存有管理者的帳號與密碼。
3. Y 高中的 NAS 內被加密的檔案是被 admin 權限所執行，而且該 NAS 預設的 admin 權限是開啟的。
4. 在 NAS 內沒有所有檔案都被加密，當檔案數量太多或是訪問多層次資料夾時，則出現加密不完全的現象。推測疑似因為 NAS 硬體資源有限與存放檔案數量過多的關係，而無法一次性將 NAS 內所有檔案加密。
5. Y 高中的 NAS 有開放給校外連線，而且該校有將 NAS 內資料夾當成網路磁碟機使用的習慣。
6. Y 高中提供勒索通知信檔案與在 NAS 內所發現的惡意程式給 TACERT 進行檢測，以利了解該勒索病毒對於受害設備進行何種攻擊行為。

二、事件檢測

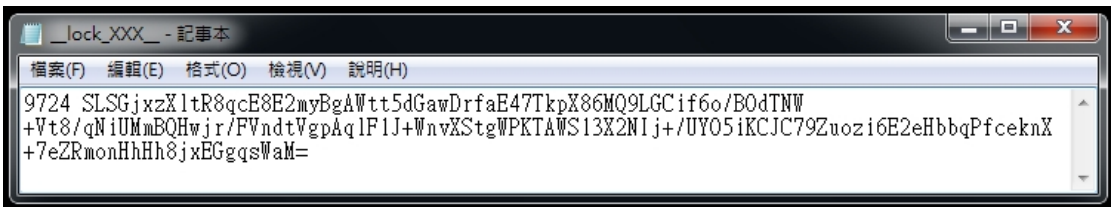
1. 首先，從學校所提供的檔案可以得知該校 NAS 被攻擊的事件時間點為 2020/12/2 上午 12:11(凌晨 12:11)。程式 Genesis_en.exe 是在 2020/12/2 上午 06:37 在 NAS 上建立，而且該程式最後一次被修改日期為 2020/11/20 下午 04:19。又該校 NAS 內檔案沒有全部被加密，由此可以推測駭客可能在 NAS 內執行第一次加密後發現檔案沒有全部被加密，而企圖想再次執行加密，故再次返回將 Genesis_en.exe 放入 NAS 內。



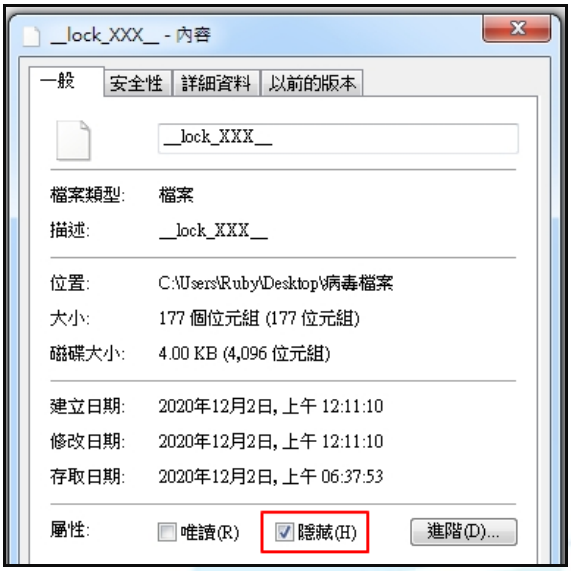
2. 檢視!HELP!.txt 的內容，駭客告訴受害者您的檔案已被加密外，也告訴受害者您的私人敏感資訊也被偷走了。駭客威脅受害者若不付贖金這些資料可能被發佈在各大媒體的即時新聞中，並要求受害者立即寫信至聯絡信箱(genesishelp@mail.ee 或 genesishelp@cock.li)。在勒索通知信最後註明該受害者的 Personal ID，該 Personal ID 為一組亂碼對應到一組數字:「47352c3f62d27b248f881a2c52b94680973aee9f394983817078336d630d956b」。



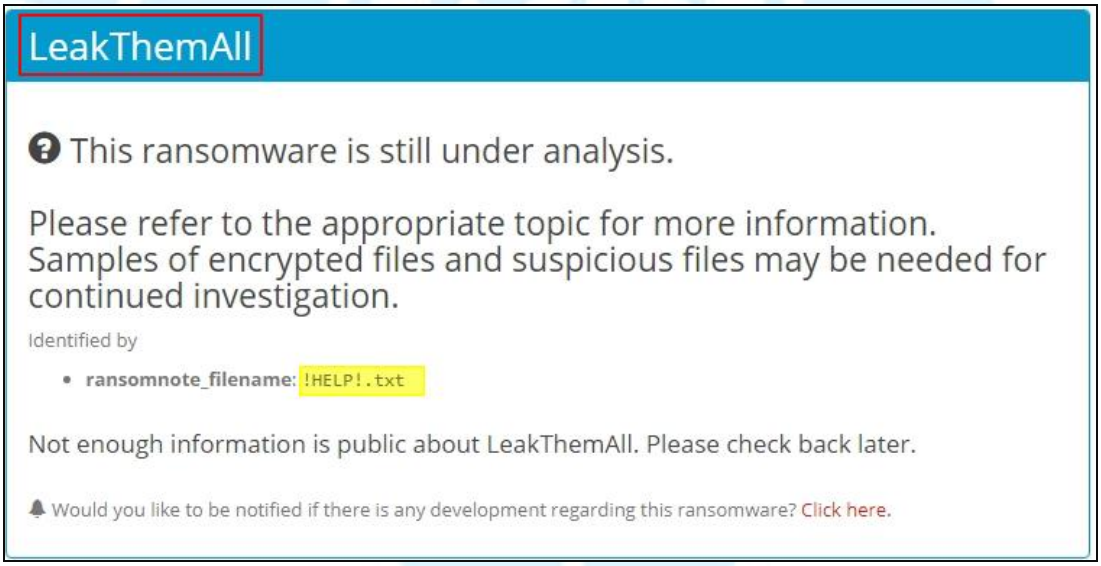
3. 檢視__lock_XXX__的內容，發現內含!HELP!.txt 內的 Personal ID 資訊。



查看__lock_XXX__的屬性發現其為一個隱藏檔。



4. 將!HELP!.txt 與__lock_XXX__上傳至 ID Ransomware 勒索病毒識別網站 (https://id-ransomware.malwarehunterteam.com)，經檢測判定為 LeakThemAll，而且該勒索病毒目前還在被研究分析中。其為新的病毒，而且尚未有解密器產生。



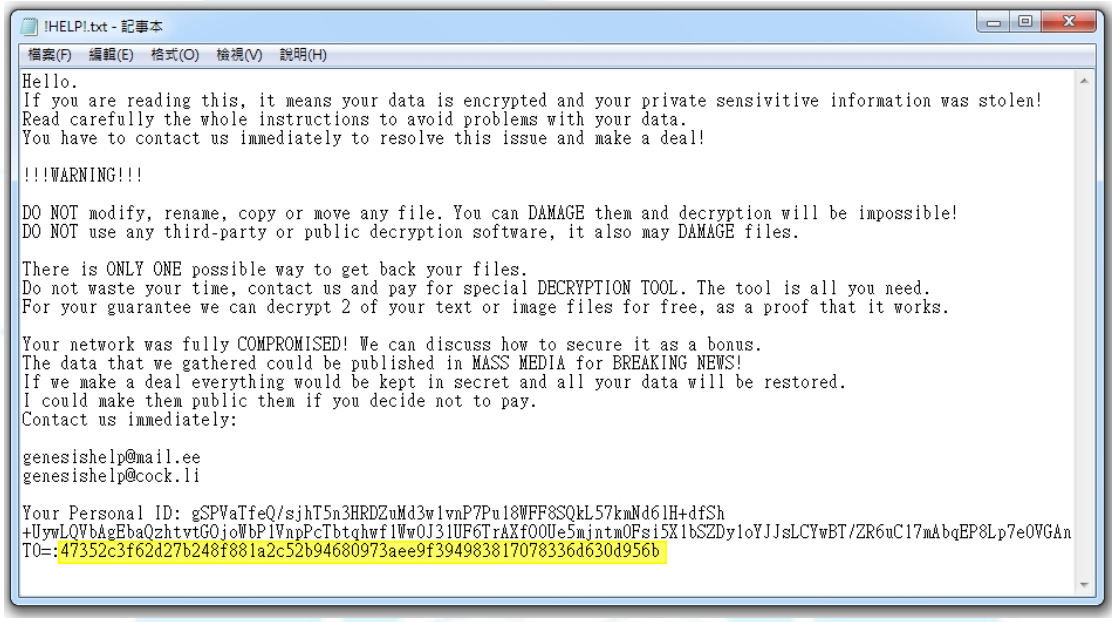
5. 將 genesis_en.exe 上傳至 Virustotal 網站檢測，發現該勒索病毒為首次上傳。經 Virustotal 檢測其惡意比例高達 45/70，而且仍有 25 家防毒軟體公司的防毒軟體無法檢測出它的存在。

Ad-Aware	Gen:Variant.Ransom.Hermes.140	AhnLab-V3	Malware/Win32.Generic.C3493871
ALYac	Gen:Variant.Ransom.Hermes.140	Antiy-AVL	Trojan/Win32.Occamy
SecureAge APEX	Malicious	Arcabit	Trojan.Ransom.Hermes.140
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	TR/FileCoder.hiflh	BitDefender	Gen:Variant.Ransom.Hermes.140
BitDefenderTheta	Gen:NN.ZexaF.34670.ImHfa871Fbni	CAT-QuickHeal	Trojanransom.Encoder
ClamAV	Win.Ransomware.Razy-9248974-0	Cynet	Malicious (score: 90)
DrWeb	Trojan.Encoder.29768	eGambit	Unsafe.AI_Score_99%
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Ransom.Hermes.140 (B)
eScan	Gen:Variant.Ransom.Hermes.140	ESET-NOD32	A Variant Of Win32/Filecoder.NXU
F-Secure	Trojan.TR/FileCoder.hiflh	FireEye	Generic.mg.6d21c44a2377fc87
Fortinet	W32/Encoder.B225!tr.ransom	GData	Gen:Variant.Ransom.Hermes.140
Gridinsoft	Ransom.Win32.Gen.dd!s2	Ikarus	Trojan-Ransom.FileCrypter
Jiangmin	Trojan.Encoder.on	Kaspersky	HEUR:Trojan-Ransom.Win32.Encoder.vho

MAX	Malware (ai Score=89)	McAfee	GenericRXAA-AA!6D21C44A2377
McAfee-GW-Edition	BehavesLike.Win32.Sality.hc	Microsoft	Ransom:Win32/Filecoder.BA!MTB
NANO-Antivirus	Trojan.Win32.Filecoder.gddbai	Panda	Trj/GdSda.A
Qihoo-360	HEUR/QVM11.1.C219.Malware.Gen	Sophos	Generic ML PUA (PUA)
Symantec	ML.Attribute.HighConfidence	Tencent	Win32.Trojan.Filecoder.Wpjl
TrendMicro	Ransom.Win32.HERMES.SMDS	TrendMicro-HouseCall	Ransom.Win32.HERMES.SMDS
VBA32	BScope.Trojan.Encoder	VIPRE	Trojan.Win32.Generic!BT
Yandex	Trojan.GenAsa!IiULxO9OIEA	Zillya	Trojan.Filecoder.Win32.10763
ZoneAlarm by Check Point	HEUR:Trojan-Ransom.Win32.Encoder.vho	Acronis	Undetected

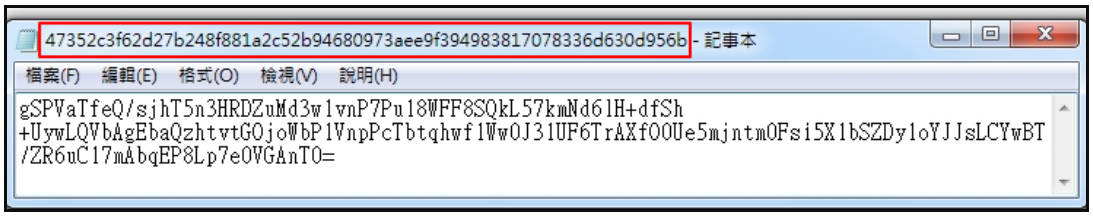
6. 進行 genesis_en.exe 的檢測，使用一台掛載網路碟機的 Win 7 32 位元主機，並且執行 genesis_en.exe (MD5: 6d21c44a2377fc871ae00106e4a0a3b7)。經執行後發現 genesis_en.exe 在原地消失。

7. 查看!HELP!.txt 內容，發現與學校所提供的!HELP!.txt 內容相同，僅 Personal ID 會隨每次執行 genesis_en.exe 而不同。這個 Personal ID 每次都會固定對應到的一組相同的數字「47352c3f62d27b248f881a2c52b94680973aee9f394983817078336d630d956b」。



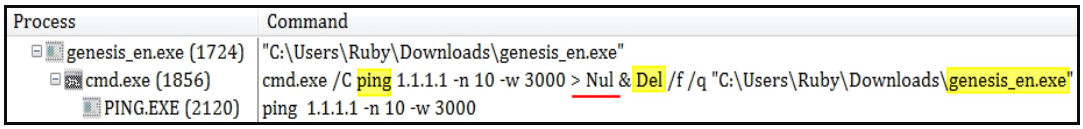
8. 在 C:\ProgramData 資料夾內發現一檔名為「47352c3f62d27b248f881a2c52b94680973aee9f394983817078336d630d956b」的檔案，它在 genesis_en.exe 執行後會先產生。之後該資料夾才出現!HELP!.txt。

檢視這個數字命名的檔案內容發現為 Personal ID，而且該檔案在主機內僅此一個。每次病毒執行後都會在這資料夾內產生相同檔名的檔案。



9. 查看檔案被加密的情形，發現所有被加密的檔案都會延伸出.genesis 的副檔名，而且被 genesis_en.exe 拜訪過的資料夾內都會產生一個!HELP!.txt。

10. 在 genesis_en.exe 執行後會呼叫 cmd.exe 來執行兩個指令。



(1) ping 1.1.1.1 –n 10 –w 3000 >Nul

在執行情形不呈現於主機螢幕上之情況下，ping Cloudflare 的 Public DNS 主機 1.1.1.1。要傳送的回應(echo)要求數目為 10 ，而且每個回覆的等候

逾時為 3000 毫秒。推測駭客此行為在確保主機是連接網路的狀態。

(2) Del /f /q "C:\Users\Ruby\Downloads\genesis_en.exe"

在系統不會提示使用者確認刪除的訊息下，強制刪除檔案 genesis_en.exe。由此可知該病毒在加密後會自我刪除本身。

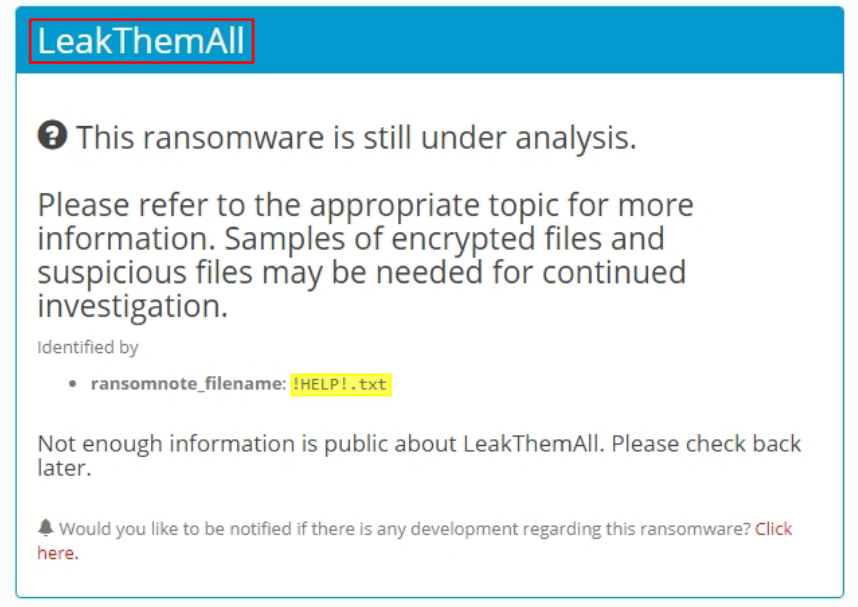
11. 在 genesis_en.exe 執行後，它會先在主機桌面產生!HELP!.txt。在加密過程中，它會對每個拜訪過的資料夾都先產生一個暫時的隱藏檔案__lock_XXX__。之後才產生!HELP!.txt 於資料夾內。在加密作業完成後，__lock_XXX__會消失。

Time of Day	Process Name	PID	Operation	Path
上午 11:11:38.6296411	genesis_en.exe	1724	CloseFile	C:\Program Files
上午 11:11:38.6299692	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Desktop\!HELP!.txt
上午 11:11:38.6306614	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Desktop\!HELP!.txt
上午 11:11:38.6315879	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Downloads__lock_XXX__
上午 11:11:38.6317237	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Downloads__lock_XXX__
上午 11:11:38.6321528	genesis_en.exe	1724	CreateFile	D:__lock_XXX__
上午 11:11:38.6323918	genesis_en.exe	1724	CloseFile	D:__lock_XXX__
上午 11:11:38.6325457	genesis_en.exe	1724	CreateFile	D:__lock_XXX__
上午 11:11:38.6326183	genesis_en.exe	1724	CloseFile	D:__lock_XXX__
上午 11:11:38.6327054	genesis_en.exe	1724	CreateFile	D:\!HELP!.txt
上午 11:11:38.6329169	genesis_en.exe	1724	CloseFile	D:\!HELP!.txt

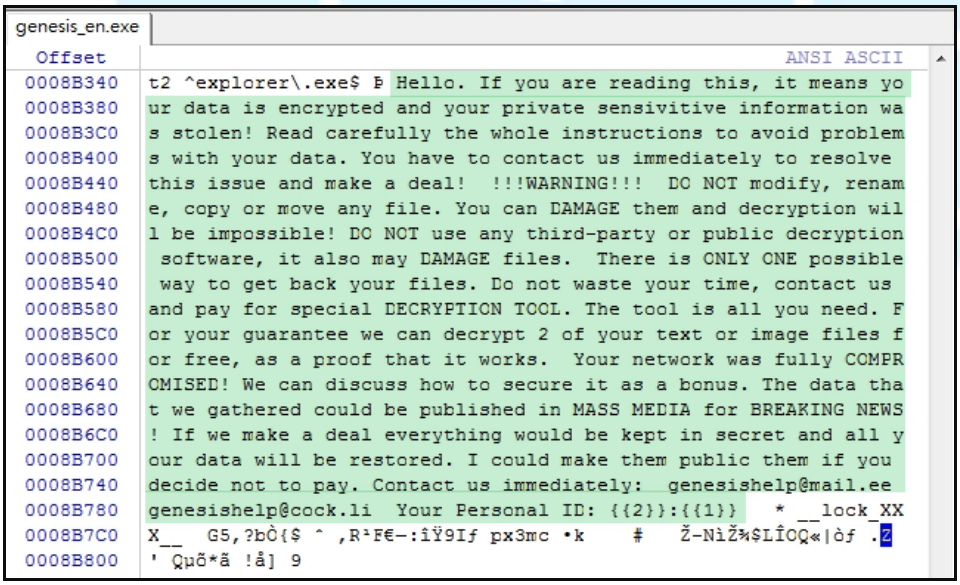
12. 檢視 genesis_en.exe 加密檔案的過程，如下圖可得知會先在 Documents 資料夾內產生__lock_XXX__，之後產生!HELP!.txt。最後開始加密第一個檔案 ABC.txt.genesis。

Time of Day	Process Name	PID	Operation	Path
上午 11:11:38.7333198	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7335742	genesis_en.exe	1724	WriteFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7336017	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7336879	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7336956	genesis_en.exe	1724	QueryBasicInformationFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7336980	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7337346	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7337434	genesis_en.exe	1724	SetBasicInformationFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7337607	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents__lock_XXX__
上午 11:11:38.7338289	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\!HELP!.txt
上午 11:11:38.7340353	genesis_en.exe	1724	WriteFile	C:\Users\Ruby\Documents\!HELP!.txt
上午 11:11:38.7340864	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents\!HELP!.txt
上午 11:11:38.7341491	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents
上午 11:11:38.7341577	genesis_en.exe	1724	QueryDirectory	C:\Users\Ruby\Documents*
上午 11:11:38.7341684	genesis_en.exe	1724	QueryDirectory	C:\Users\Ruby\Documents
上午 11:11:38.7349332	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7349831	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7350562	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7350640	genesis_en.exe	1724	QueryNetworkOpenInformationFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7350670	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7351361	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7351428	genesis_en.exe	1724	QueryNetworkOpenInformationFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7351448	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7352231	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt.genesis
上午 11:11:38.7352696	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7352793	genesis_en.exe	1724	QueryAttributeTagFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7352861	genesis_en.exe	1724	QueryBasicInformationFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7353265	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents
上午 11:11:38.7353495	genesis_en.exe	1724	SetRenameInformationFile	C:\Users\Ruby\Documents\ABC.txt
上午 11:11:38.7355758	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents
上午 11:11:38.7356015	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents\ABC.txt.genesis
上午 11:11:38.7357408	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt.genesis
上午 11:11:38.7358383	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt.genesis
上午 11:11:38.7358605	genesis_en.exe	1724	QueryNetworkOpenInformationFile	C:\Users\Ruby\Documents\ABC.txt.genesis
上午 11:11:38.7358925	genesis_en.exe	1724	CloseFile	C:\Users\Ruby\Documents\ABC.txt.genesis
上午 11:11:38.7359614	genesis_en.exe	1724	CreateFile	C:\Users\Ruby\Documents\ABC.txt.genesis

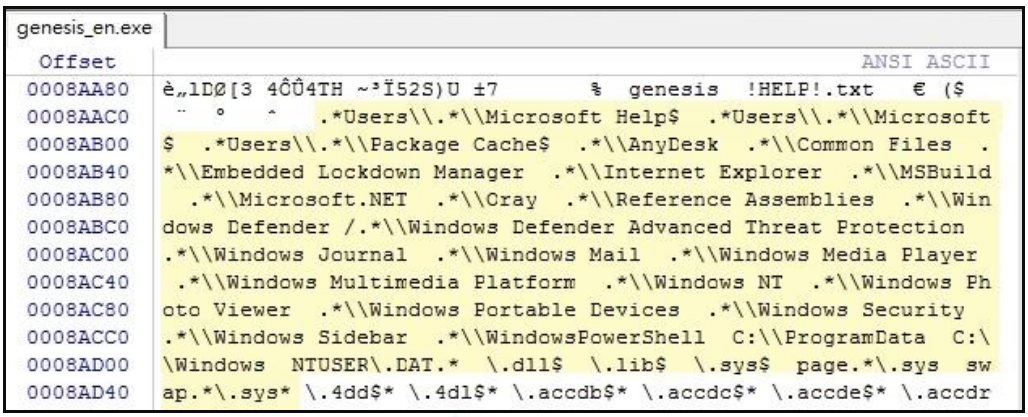
13. 將!HELP!.txt 與一個被加密的 ABC.txt.genesis 檔案上傳至 ID Ransomware 勒索病毒識別網站，經檢測判定為 LeakThemAll，而且該勒索病毒目前仍在被研究分析中、尚未有解密器。與前面學校所提供檔案的判斷內容相同，可確認 genesis_en.exe 為此事件的勒索病毒程式。

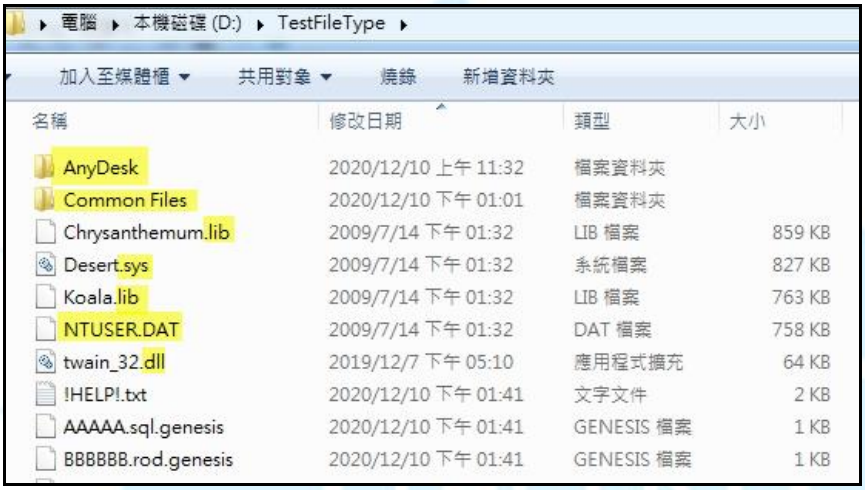


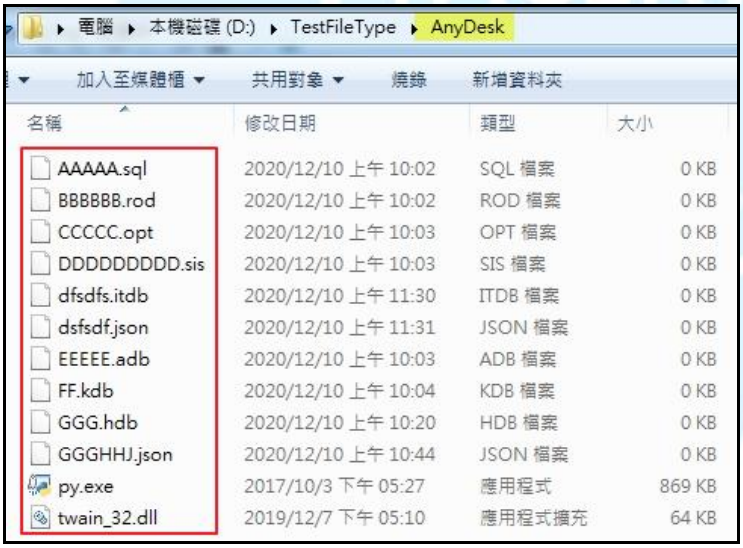
14. 對 genesis_en.exe 的程式內容進行 HEX 分析，發現內含!HELP!.txt 的內容。



15. 從 genesis_en.exe 程式的 HEX 分析內容與實際檢測發現，該程式不會對下圖中所列資料夾內檔案、NTUSER.DAT 與副檔名為.dll、.lib、.sys 的檔案進行加密。例如:AnyDesk(遠端桌面連線用)疑似是駭客為方便遠端連線而保留的資料夾。





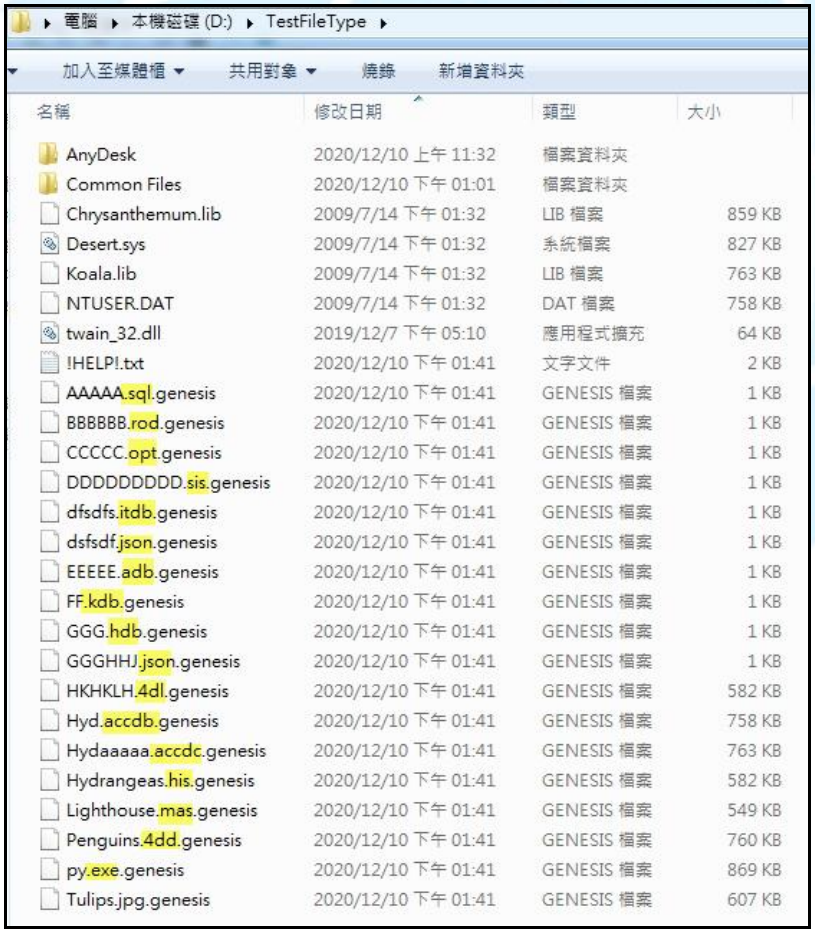


16. 從程式 genesis_en.exe 的 HEX 內容發現下圖所列的資料庫程式或資料檔案用的副檔名，推測該程式可能會搜尋主機內是否存在這些檔案。

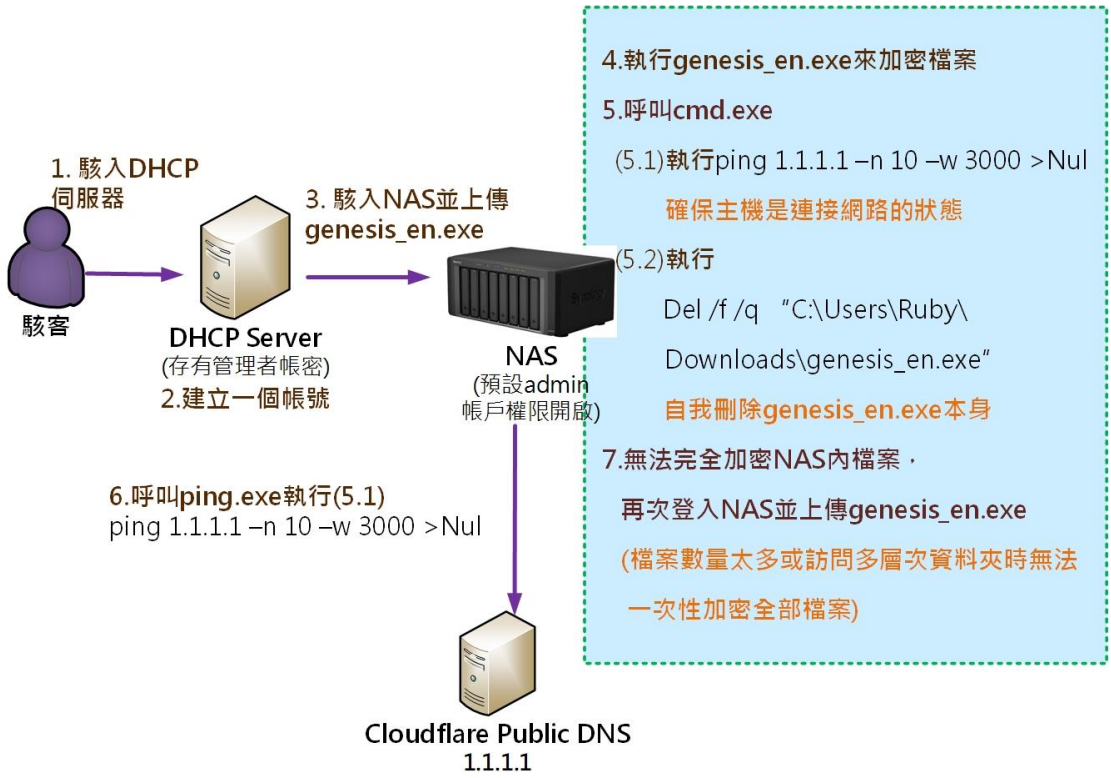
genesis_en.exe

Offset	ANSI ASCII
0008AD00	\Windows NTUSER\.DAT.* \.dll$ \.lib$ \.sys$ page.*\.sys sw
0008AD40	ap.*\.sys* \.4dd$* \.4dl$* \.accdb$* \.accdc$* \.accde$* \.accdr
0008AD80	$* \.accdt$* \.accft$* \.adb$* \.ade$* \.adf$* \.adp$* \.alf$* \
0008ADC0	.arm$* \.arz$* \.ask$* \.bak$* \.bson$* \.btr$* \.cat$* \.cdb$*
0008AE00	\.ckp$* \.cma$* \.cnf$* \.cpd$* \.crypt12$* \.crypt8$* \.crypt9$
0008AE40	* \.dacpac$* \.dad$* \.dadiagrams$* \.daschema$* \.db$* \.db-shm
0008AE80	$* \.db-wal$* \.db3$* \.dbc$* \.dbf$* \.dbs$* \.dbt$* \.dbv$* \.
0008AEC0	dbx$* \.dcb$* \.dct$* \.dcx$* \.ddl$* \.dlis$* \.dmp$* \.dp1$* \
0008AF00	.dqy$* \.dsk$* \.dsn$* \.dtsx$* \.dxl$* \.eco$* \.ecx$* \.edb$*
0008AF40	\.epim$* \.fcd$* \.fdb$* \.fic$* \.fm5$* \.fmp$* \.fmp12$* \.fmp
0008AF80	sl$* \.fol$* \.fp3$* \.fp4$* \.fp5$* \.fp7$* \.fpt$* \.frm$* \.g
0008AFC0	db$* \.grdb$* \.gwi$* \.hdb$* \.his$* \.ib$* \.ibc$* \.ibd$* \.i
0008B000	bz$* \.idb$* \.ihx$* \.ism$* \.itdb$* \.itw$* \.jet$* \.json$* \
0008B040	.jtx$* \.kdb$* \.kexi$* \.kexic$* \.kexis$* \.ldf$* \.lgc$* \.lw
0008B080	x$* \.maf$* \.maq$* \.mar$* \.marshal$* \.mas$* \.mav$* \.mdb$*
0008B0C0	\.mdf$* \.mpd$* \.mrg$* \.mud$* \.mwb$* \.myd$* \.myi$* \.mysql$
0008B100	* \.ndf$* \.nnt$* \.nrmlib$* \.ns2$* \.ns3$* \.ns4$* \.nsf$* \.n
0008B140	v$* \.nv2$* \.nwdb$* \.nyf$* \.odb$* \.opt$* \.oqy$* \.ora$* \.o
0008B180	rx$* \.owc$* \.p96$* \.p97$* \.pan$* \.pdb$* \.pdm$* \.phl$* \.p
0008B1C0	nz$* \.qbquery$* \.qry$* \.qvd$* \.rbf$* \.rctd$* \.rod$* \.rodx
0008B200	$* \.rpd$* \.rsd$* \.rul$* \.sal$* \.sas7bdat$* \.sbf$* \.scx$*
0008B240	\.sdb$* \.sdc$* \.sdf$* \.sis$* \.spq$* \.sql$* \.sqlite$* \.sql
0008B280	ite3$* \.sqlitedb$* \.sqr$* \.te$* \.teacher$* \.tmd$* \.tps$* \
0008B2C0	.trc$* \.trm$* \.udb$* \.udl$* \.usr$* \.v12$* \.vis$* \.vpd$* \
0008B300	.vvv$* \.wdb$* \.wmdb$* \.wrk$* \.xdb$* \.xld$* \.xmlff$2 svchos
0008B340	t2 ^explorer\.exe$ Þ Hello. If you are reading this, it means yo

經檢測發現這些副檔名的檔案是會被 genesis_en.exe 加密，並沒有排除。



三、事件攻擊行為示意圖



1. 駭客從校外駭入 DHCP 伺服器 。
2. 駭客在 DHCP 伺服器上建立一個帳號。
3. 駭客駭入 NAS 並上傳惡意程式 genesis_en.exe 至 NAS。
4. 執行 genesis_en.exe 進行檔案加密作業。

   (所拜訪的資料夾會先產生__lock_XXX__，之後產生!HELP!.txt。)
5. 呼叫 cmd.exe 來執行兩個指令。

   (5.1)執行 ping 1.1.1.1 –n 10 –w 3000 >Nul 來確保主機是連接網路的狀態。

   (5.2)執行 Del /f /q "C:\Users\Ruby\Downloads\genesis_en.exe"來刪除 genesis_en.exe 本身(在系統不會提示使用者確認刪除的訊息下，強制刪除檔案 genesis_en.exe。)。
6. 呼叫 ping.exe 來執行(5.1)

   (在執行情形不呈現於主機螢幕上之情況下，ping Cloudflare 的 Public DNS 主機 1.1.1.1。)。

7. 由於無法完全加密 NAS 內檔案，駭客再次登入 NAS 並且上傳 genesis_en.exe。(因 NAS 硬體資源有限，當檔案數量太多或是訪問多層次資料夾時無法一次性加密全部檔案。)

四、總結與建議

1. 近期新發現的 LeakTheMall 勒索軟體（又名 LeakThemAll）是一種資料鎖定病毒，最早是由網路安全研究員 Amigo-A 發現的。
2. 它會將您的文件副檔名延伸更改為.crypt、.montana 或.beijing，而最近新型變種的副檔名是.genesis。
3. 該變種病毒.genesis 執行後除加密檔案外，會 ping Public DNS 主機 1.1.1.1 來確保網路連線是開啟的狀態，並且加密作業完成後會自我刪除本身。
4. 它會固定在 C:\ProgramData 資料夾內存放固定數字檔名的 Personal ID 檔案。
5. 該病毒在加密過程中對於所拜訪的資料夾會先產生__lock_XXX__，之後產生!HELP!.txt。
6. genesis_en.exe 於 NAS 上建立時間為加密時間之後，推測駭客可能因為 NAS 硬體資源有限、檔案數量太多與資料夾多層次的原因，導致無法一次性完成加密，故想再次加密而第二次上傳程式至 NAS。
7. 該病毒有預設一個排除的資料夾、NTUSER.DAT 與副檔名為.dll、.lib、.sys 等檔案類型的名單，符合名單上所列條件的檔案都不會被加密。
8. 該病毒程式內有一些資料庫程式或資料檔案用的副檔名，推測該程式可能會搜尋主機內是否存在這些檔案。這些副檔名的檔案是會被 genesis_en.exe 加密，並沒有排除。
9. 對於此勒索病毒的預防除了平時做好資料備份外，建議在 NAS 的管理上加強下列項目:

(1.)校外連線存取需管控連線來源。

(2.)建議不要隨意開啟不明來源的檔案。

(3.)避免將 NAS 內的資料夾設為主機的網路磁碟機。

(4.)定期更新 NAS 的修補程式。

(5.)請勿使用原廠的預設帳戶與密碼管理 NAS。