TLP:WHITE

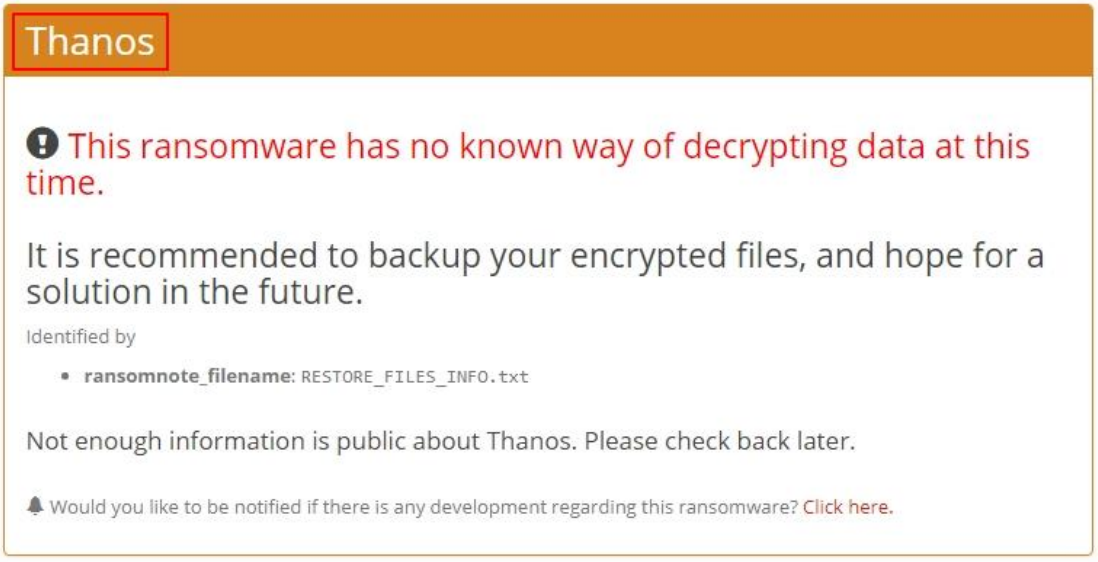
勒索病毒 Thanos 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2021 年 03 月

一、事件簡介

1. 在 2021/2 初某學校在凌晨 2:00~5:00 期間遭受勒索軟體的攻擊，造成 5 台行政用主機內檔案被加密。
2. 這些受害主機有掛載網路磁碟機的資料夾，但資料夾內檔案沒有被加密。
3. 在受害主機上無任何防毒軟體，疑似被卸載或未安裝防毒軟體。
4. 經檢測發現這些受害主機的勒索病毒特徵都相同。被加密的檔案之副檔名皆為 containers，而且都有兩種檔案類型的勒索通知信(txt 檔與 hta 檔)。
5. 這些主機內的勒索通知信與被加密的檔案經 ID Ransomware 勒索軟體識別網站(https://id-ransomware.malwarehunterteam.com)檢測，每台主機判定的結果皆為 Thanos，而且該勒索軟體目前尚未有解密器。

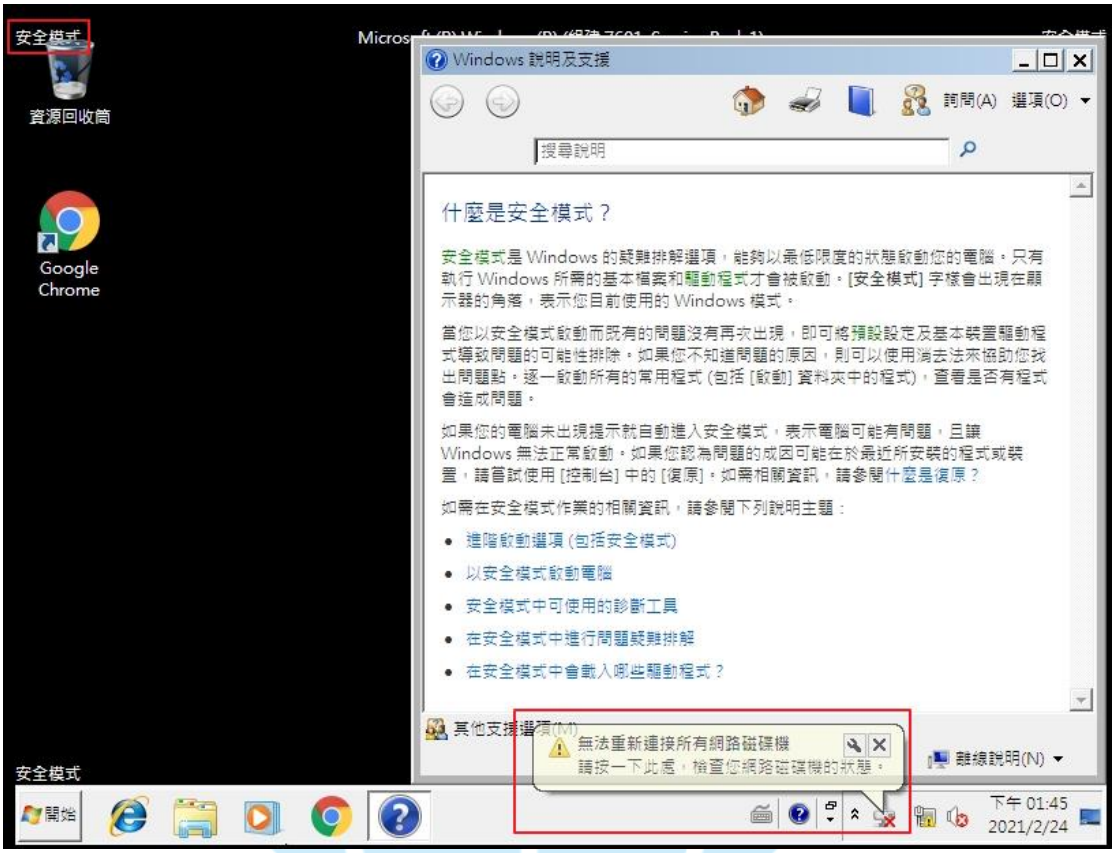


6. 為了瞭解勒索軟體 Thanos 的攻擊行為，本中心取得該類型勒索軟體的樣本後進行檢測。

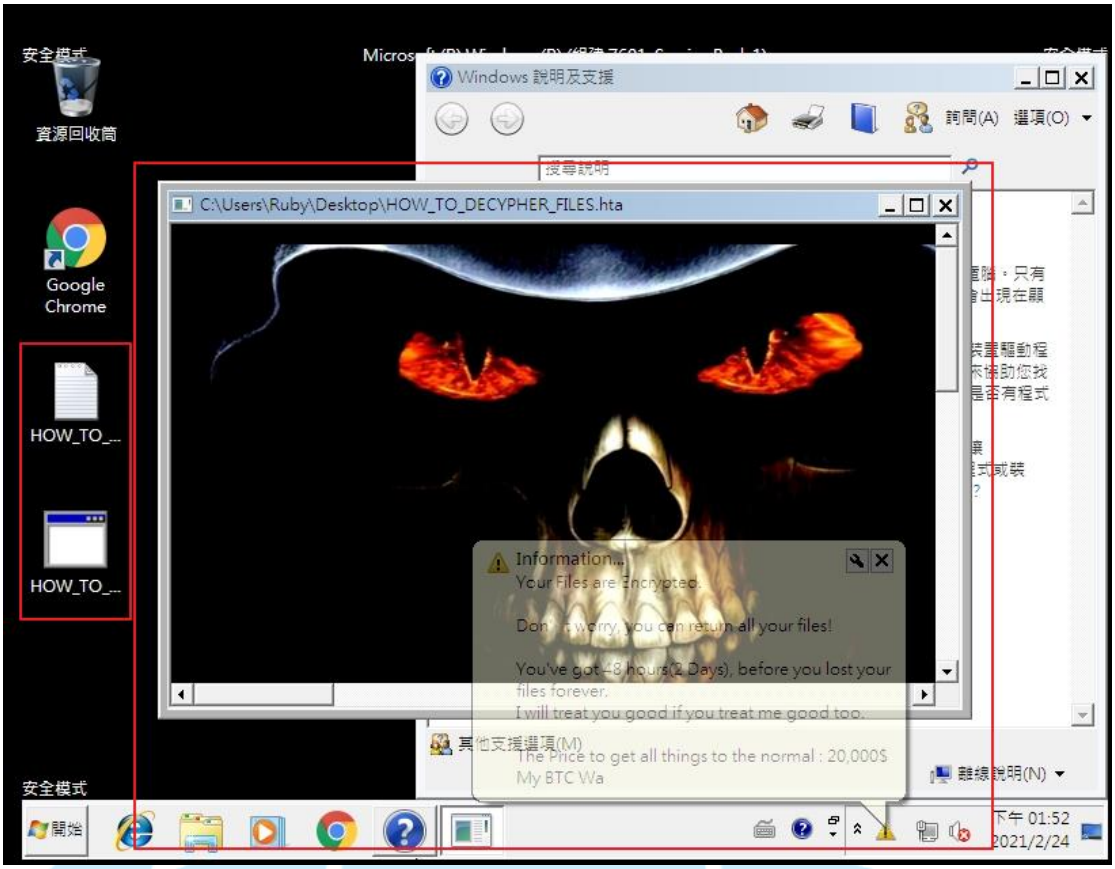
二、事件檢測

1. 首先，使用一台有掛載網路磁碟機之資料夾的 Windows 7 主機，接著將樣本 6a50.exe 置於主機上執行。

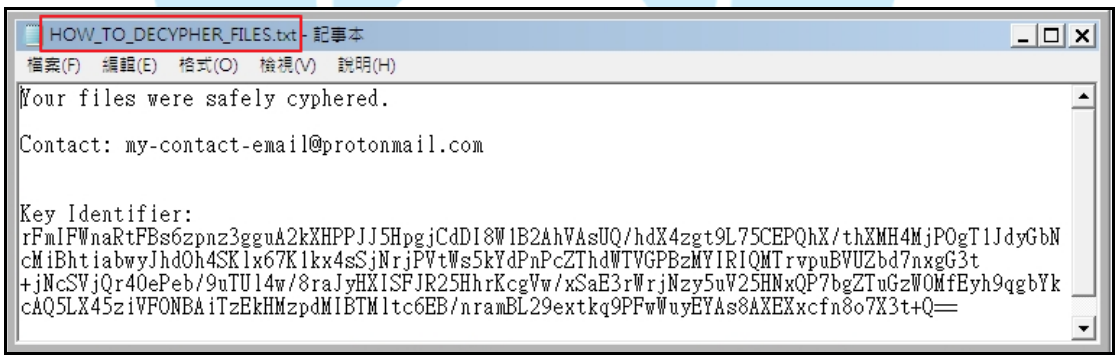
2. 執行 6a50.exe 後主機會立即重新開機。在開機完後主機進入安全模式，而且無法連接網路磁碟機。



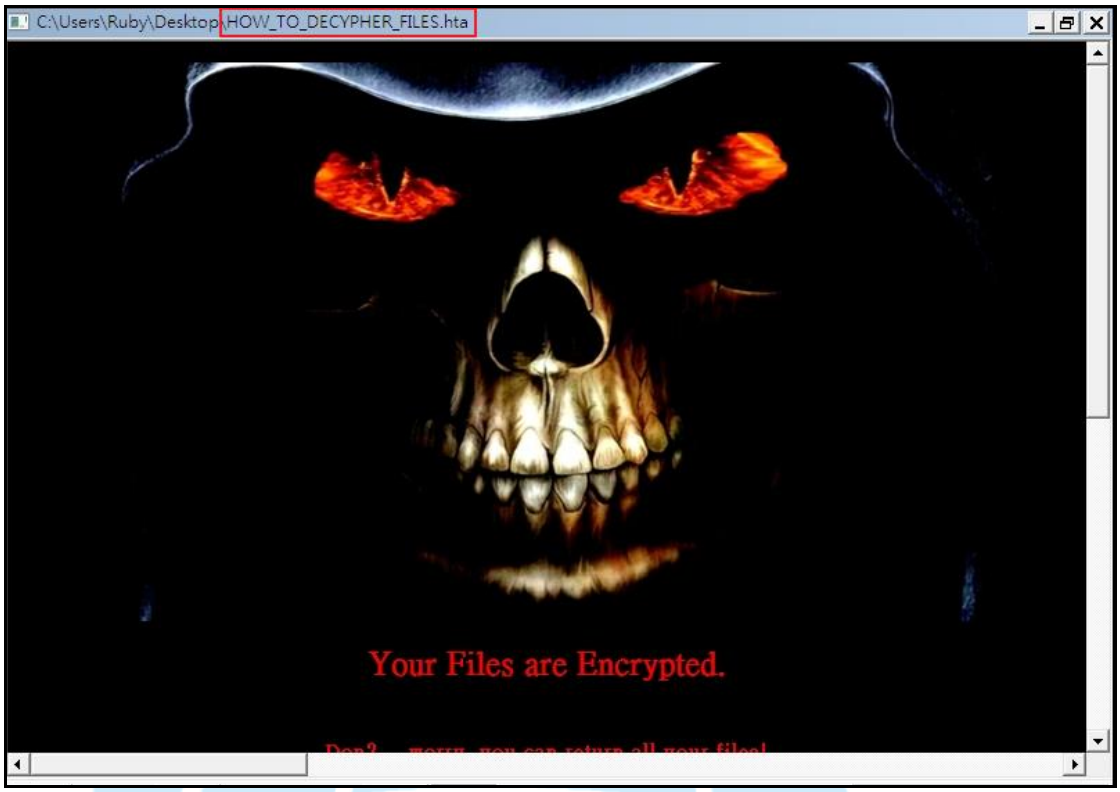
在登入安全模式後不久，桌面會出現勒索通知信 HOW_TO_DECYPHER_FILES.hta 的視窗畫面與 Information 提醒視窗，並且在桌面上也產生兩個不同檔案類型的勒索通知信檔案(txt 檔與 hta 檔)。



3. 查看 HOW_TO_DECYPHER_FILES.txt 的內容，發現駭客僅簡短地告訴受害者你的檔案已被安全地加密，並且提供了駭客的聯絡信箱。最後，文字檔內有識別這個受害主機的 Key Identifier。

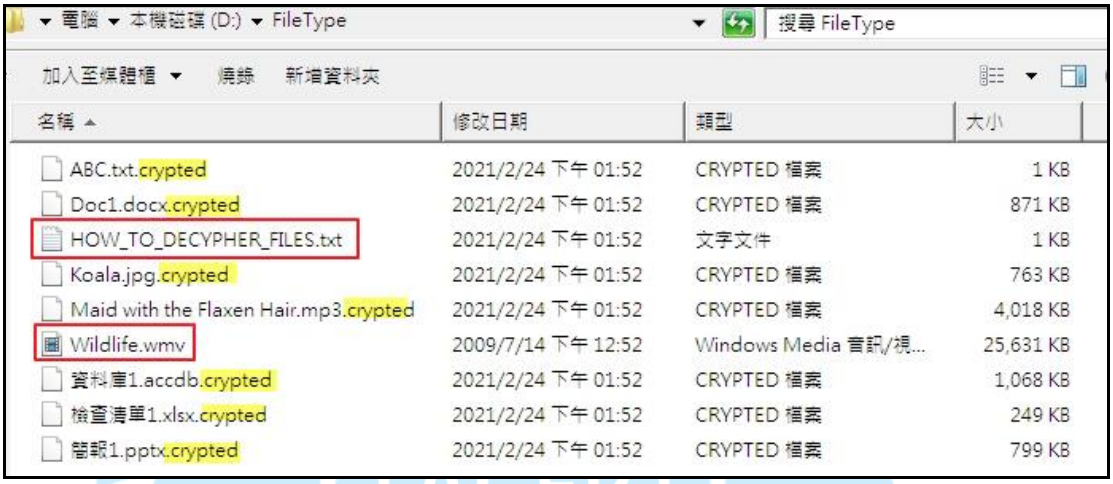


4. 檢視 HOW_TO_DECYPHER_FILES.hta 的內容，發現在主機進入安全模式後桌布大小變小。因此受害者一開始僅會看到一個鬼臉(如下圖)與「Your Files are Encrypted」，接著往下查看.hta 檔內容才會看到勒索通知信內文。

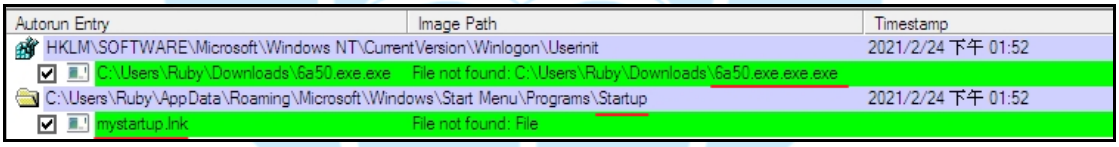


在 hta 檔的勒索通知信內文中，駭客告訴受害者不要擔心，只要在 48 小時內付款就可以還原檔案，否則檔案將遺失。駭客也提供比特幣錢包的 ID 資訊與聯絡信箱給受害者，並且告訴受害者還原這些被加密的檔案需要兩萬美金。

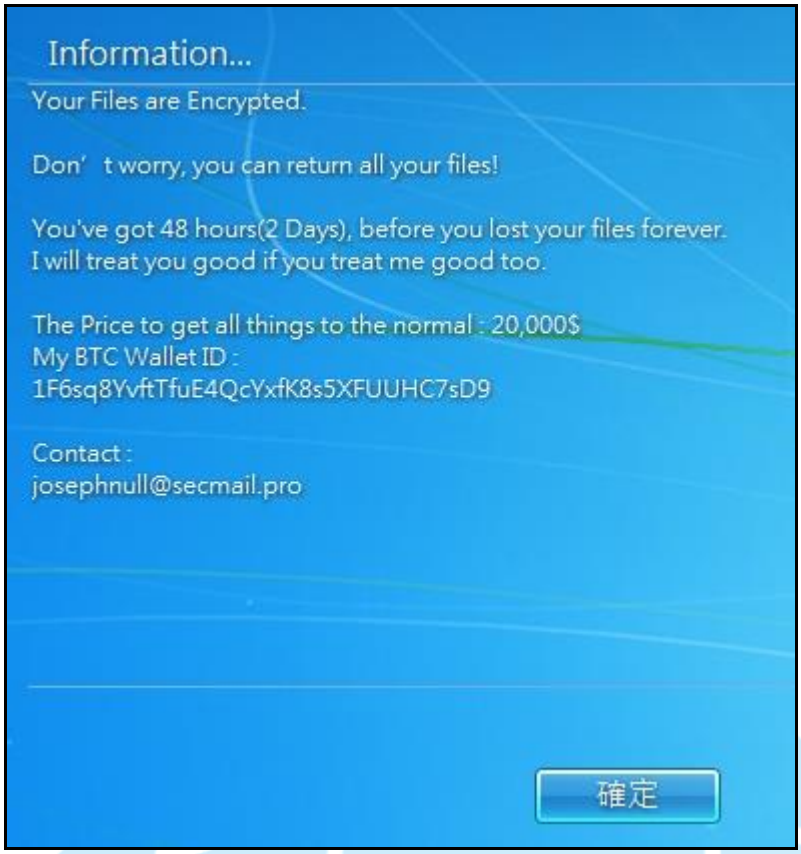
5. 檢視主機內檔案被加密的情形，發現除了 C:\windows 與 C:\program files 內的檔案沒被加密外，大部分的檔案都被加密了。被加密的檔案其副檔名為.crypted，而且在每個被加密檔案的資料夾內都有一個勒索通知信檔案 HOW_TO_DECYPHER_FILES.txt。在這些被加密的檔案中，發現.wmv 的影片檔案沒有被加密，推測該勒索軟體應該對於加密哪些類型的檔案有設定範圍。



6. 檢視主機的開機後程序，發現有兩個檔案 6a50.exe 與 mystartup.lnk 遺失。查看 6a50.exe 原來所在資料夾，發現在執行後該檔案已消失，推測該勒索軟體 Thanos 具有自我刪除本身的功能。



7. 當主機再次重新開機後，會出現一個 Information 的訊息。在按下確定按鈕後才出現登入畫面，登入後主機已不是安全模式。Information 訊息內容與 HOW_TO_DECYPHER_FILES.hta 的內容大同小異。



8. 執行 6a50.exe 後會先呼叫 powershell.exe，接著會執行 net.exe(net1.exe)、sc.exe、vssadmin.exe 、taskkill.exe、cmd.exe Mshta.exe、 bcdedit.exe、cmd.exe(PING.EXE、fsutil.exe)與 cmd.exe(Choice.exe)等程序。

(1) 呼叫 powershell.exe 來執行「"powershell" Get-MpPreference –verbose」，以取得 Windows Defender 當前的設置內容，來繞過 Windows defender 的檢測。

Process	Command
6a50.exe (1412)	C:\Users\Ruby\Downloads\6a50.exe
powershell.exe (1536)	"powershell" Get-MpPreference -verbose

(2) 陸續執行 net.exe 來呼叫 net1.exe 共 36 次，以停止 36 種防毒軟體的服務程序。

Process	Command
net.exe (1720)	"net.exe" stop avpsus /y
net1.exe (292)	C:\Windows\system32\net1 stop avpsus /y
net.exe (1728)	"net.exe" stop McAfeeDLPAgentService /y
net1.exe (2416)	C:\Windows\system32\net1 stop McAfeeDLPAgentService /y
net.exe (1744)	"net.exe" stop mfewc /y
net1.exe (2400)	C:\Windows\system32\net1 stop mfewc /y
net.exe (1752)	"net.exe" stop BMR Boot Service /y
net1.exe (384)	C:\Windows\system32\net1 stop BMR Boot Service /y
net.exe (1768)	"net.exe" stop NetBackup BMR MTFTP Service /y
net1.exe (2688)	C:\Windows\system32\net1 stop NetBackup BMR MTFTP Service /y
net.exe (1776)	"net.exe" stop DefWatch /y
net1.exe (2432)	C:\Windows\system32\net1 stop DefWatch /y
net.exe (1792)	"net.exe" stop ccEvtMgr /y
net1.exe (2736)	C:\Windows\system32\net1 stop ccEvtMgr /y
net.exe (1800)	"net.exe" stop ccSetMgr /y
net1.exe (2620)	C:\Windows\system32\net1 stop ccSetMgr /y
net.exe (1812)	"net.exe" stop SavRoam /y
net1.exe (2744)	C:\Windows\system32\net1 stop SavRoam /y
net.exe (1828)	"net.exe" stop RTVscan /y
net1.exe (2648)	C:\Windows\system32\net1 stop RTVscan /y
net.exe (1836)	"net.exe" stop QBFCService /y
net1.exe (2628)	C:\Windows\system32\net1 stop QBFCService /y
net.exe (1852)	"net.exe" stop QBIDPService /y
net1.exe (2696)	C:\Windows\system32\net1 stop QBIDPService /y
net.exe (1860)	"net.exe" stop Intuit.QuickBooks.FCS /y
net1.exe (2660)	C:\Windows\system32\net1 stop Intuit.QuickBooks.FCS /y
net.exe (1868)	"net.exe" stop QBCFMonitorService /y
net1.exe (2772)	C:\Windows\system32\net1 stop QBCFMonitorService /y
net.exe (1876)	"net.exe" stop YooBackup /y
net1.exe (2824)	C:\Windows\system32\net1 stop YooBackup /y

Process	Command
net.exe (1888)	"net.exe" stop YooIT /y
net1.exe (2892)	C:\Windows\system32\net1 stop YooIT /y
net.exe (1896)	"net.exe" stop zhudongfangyu /y
net1.exe (2728)	C:\Windows\system32\net1 stop zhudongfangyu /y
net.exe (1904)	"net.exe" stop stc_raw_agent /y
net1.exe (2784)	C:\Windows\system32\net1 stop stc_raw_agent /y
net.exe (1936)	"net.exe" stop VSNAPVSS /y
net1.exe (2840)	C:\Windows\system32\net1 stop VSNAPVSS /y
net.exe (1952)	"net.exe" stop VeeamTransportSvc /y
net1.exe (2672)	C:\Windows\system32\net1 stop VeeamTransportSvc /y
net.exe (1964)	"net.exe" stop VeeamDeploymentService /y
net1.exe (2720)	C:\Windows\system32\net1 stop VeeamDeploymentService /y
net.exe (1972)	"net.exe" stop VeeamNFSSvc /y
net1.exe (2704)	C:\Windows\system32\net1 stop VeeamNFSSvc /y
net.exe (1980)	"net.exe" stop veeam /y
net1.exe (2832)	C:\Windows\system32\net1 stop veeam /y
net.exe (1988)	"net.exe" stop PDVFSService /y
net1.exe (2612)	C:\Windows\system32\net1 stop PDVFSService /y
net.exe (1996)	"net.exe" stop BackupExecVSSProvider /y
net1.exe (2604)	C:\Windows\system32\net1 stop BackupExecVSSProvider /y
net.exe (2004)	"net.exe" stop BackupExecAgentAccelerator /y
net1.exe (2680)	C:\Windows\system32\net1 stop BackupExecAgentAccelerator /y
net.exe (2020)	"net.exe" stop BackupExecAgentBrowser /y
net1.exe (2848)	C:\Windows\system32\net1 stop BackupExecAgentBrowser /y
net.exe (2032)	"net.exe" stop BackupExecDiveciMediaService /y
net1.exe (2792)	C:\Windows\system32\net1 stop BackupExecDiveciMediaService /y
net.exe (112)	"net.exe" stop BackupExecJobEngine /y
net1.exe (2864)	C:\Windows\system32\net1 stop BackupExecJobEngine /y
net.exe (252)	"net.exe" stop BackupExecManagementService /y
net1.exe (2760)	C:\Windows\system32\net1 stop BackupExecManagementService /y
net.exe (280)	"net.exe" stop BackupExecRPCService /y
net1.exe (2872)	C:\Windows\system32\net1 stop BackupExecRPCService /y

Process	Command
net.exe (308)	"net.exe" stop AcrSch2Svc /y
net1.exe (2856)	C:\Windows\system32\net1 stop AcrSch2Svc /y
net.exe (312)	"net.exe" stop AcronisAgent /y
net1.exe (2800)	C:\Windows\system32\net1 stop AcronisAgent /y
net.exe (356)	"net.exe" stop CASAD2DWebSvc /y
net1.exe (2816)	C:\Windows\system32\net1 stop CASAD2DWebSvc /y
net.exe (380)	"net.exe" stop CAARCUpdateSvc /y
net1.exe (2752)	C:\Windows\system32\net1 stop CAARCUpdateSvc /y
net.exe (472)	"net.exe" stop sophos /y
net1.exe (2900)	C:\Windows\system32\net1 stop sophos /y

(3) 為防止惡意軟體 Thanos 被終止，該惡意軟體還執行以下服務控制和

taskkill 命令。利用執行 sc.exe 來修改註冊表與服務控制管理器資料庫中服務條的目的值，以關閉 4 個非關鍵服務，其中 3 個為與 SQL 有關的服務。

Process	Command
sc.exe (620)	"sc.exe" config SQLTELEMETRY start= disabled
sc.exe (984)	"sc.exe" config SQLTELEMETRY$ECWDB2 start= disabled
sc.exe (1104)	"sc.exe" config SQLWriter start= disabled
sc.exe (1292)	"sc.exe" config SstpSvc start= disabled

(4) 執行 taskkill.exe 來中止 3 個執行中的程序(mspub.exe、mydesktopqos.exe 與 mydesktopservice.exe)。

Process	Command
taskkill.exe (1348)	"taskkill.exe" /IM mspub.exe /F
taskkill.exe (2132)	"taskkill.exe" /IM mydesktopqos.exe /F
taskkill.exe (2148)	"taskkill.exe" /IM mydesktopservice.exe /F

(5) 該惡意軟體還執行 vssadmin.exe 來刪除所有影子副本與調整陰影複製儲存區關聯的大小上限。

Process	Command
vssadmin.exe (2164)	"vssadmin.exe" Delete Shadows /all /quiet
vssadmin.exe (2180)	"vssadmin.exe" resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin.exe (2196)	"vssadmin.exe" resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin.exe (2212)	"vssadmin.exe" resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin.exe (2284)	"vssadmin.exe" resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin.exe (2340)	"vssadmin.exe" resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin.exe (2372)	"vssadmin.exe" resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin.exe (2392)	"vssadmin.exe" resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin.exe (2424)	"vssadmin.exe" resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin.exe (2456)	"vssadmin.exe" resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin.exe (2472)	"vssadmin.exe" resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin.exe (2496)	"vssadmin.exe" resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin.exe (2520)	"vssadmin.exe" resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin.exe (2536)	"vssadmin.exe" Delete Shadows /all /quiet

(6) 執行 cmd.exe(2572)來清空資源回收桶內所有檔案，執行 mshta.exe 來顯示勒索通信的.hta 檔內容，透過 bcdedit.exe 來下達在開機時取消進入安全模式的指令。

Process	Command
cmd.exe (2572)	"cmd.exe" /c rd /s /q %SYSTEMDRIVE%\$Recycle.bin
mshta.exe (3664)	"C:\Windows\System32\mshta.exe" C:\Users\Ruby\Desktop\HOW_TO_DECYPHER_FILES.hta
bcdedit.exe (3680)	"bcdedit.exe" /deletevalue {default} safeboot

(7) 執行 cmd.exe(3688)呼叫 PING.EXE 來將 ping 指令輸出重定向至無效設備，而不是控制台。之後 cmd.exe(3688)會呼叫 fsutil.exe 來使用空資料覆蓋檔案中的資料，從檔案的第 0 個字節開始覆蓋，覆蓋長度為 524288 個

字節。最後在不會跳出提示訊息的安靜模式下強制刪除檔案。

Process	Command
cmd.exe (3688)	"cmd.exe" /C ping 127.0.0.7 -n 3 > Nul & fsutil file setZeroData offset=0 length=524288 "%s" & Del /f /q "%s"
PING.EXE (3788)	ping 127.0.0.7 -n 3
fsutil.exe (3904)	fsutil file setZeroData offset=0 length=524288 "%s"

(8) 執行 cmd.exe(3708)呼叫 choice.exe 來在指定時間內進行只有一個 Y 選項的選擇，最後會刪除惡意軟體 6a50.exe。

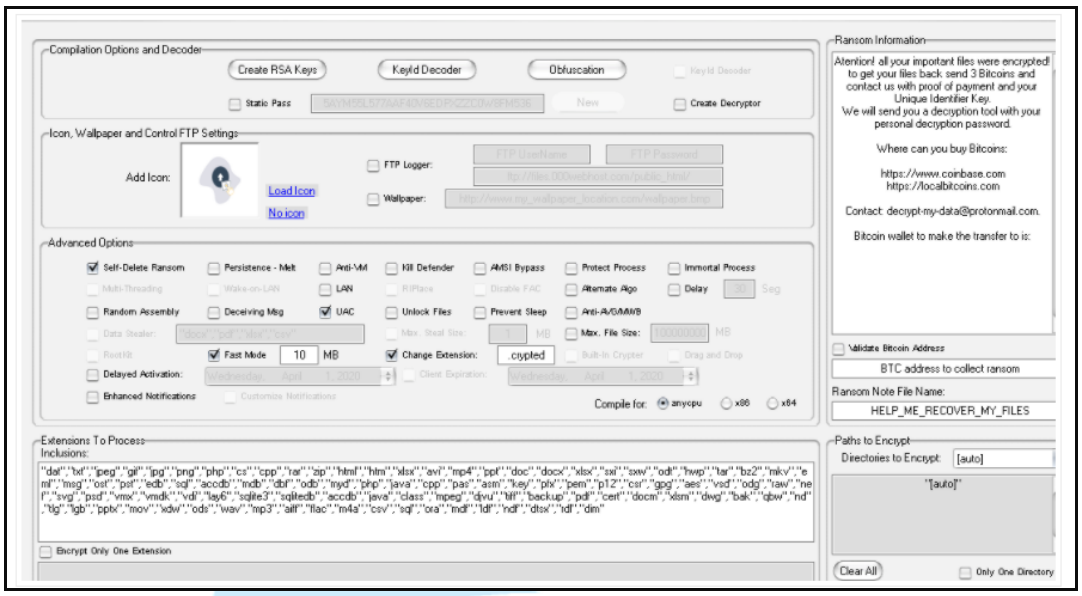
Process	Command
cmd.exe (3708)	"C:\Windows\System32\cmd.exe" "/C choice /C Y /N /D Y /T 3 & Del "C:\Users\Ruby\Downloads\6a50.exe
choice.exe (3808)	choice /C Y /N /D Y /T 3

9. 6a50.exe 經 Virustotal 檢測其惡意比例很高，為 60/71。少數防毒軟體公司以 Thanos 命名它。大多數防毒軟體可偵測出樣本 6a50.exe 所在。

ALYac	Trojan.Ransom.Thanos	Antiy-AVL	Trojan[Ransom]/Win32.Generic
SecureAge APEX	Malicious	Arcabit	Trojan.Barys.D6456
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	TR/Dropper.Gen2	BitDefender	Gen:Variant.Barys.25686
BitDefenderTheta	AI:Packer.0C318DE31F	CAT-QuickHeal	Trojanransom.Generic
ClamAV	Win.Ransomware.Thanos-9755595-0	Comodo	Malware@#3frppywzwg7kl

Sophos	Mal/Generic-R + Mal/Hakbit-A	Symantec	Ransom.Cryptolocker
Tencent	Win32.Trojan.Generic.Egen	TrendMicro	Ransom.MSIL.THANOS.SM
TrendMicro-HouseCall	Ransom.MSIL.THANOS.SM	VBA32	TScope.Trojan.MSIL

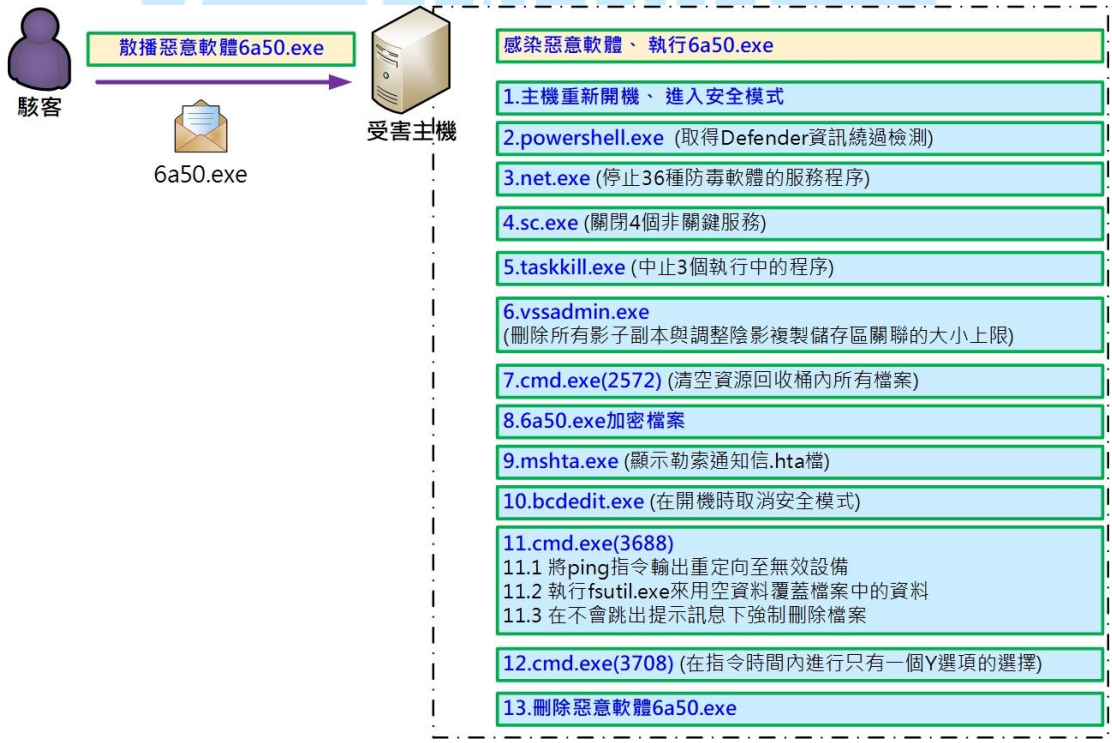
Thanos ransomware builder 具有 43 種配置項目，可以依配置項目產生不同特徵的 Thanos 變種樣本，其中具有繞過防毒軟體偵測的配置選項。 因此，防毒軟體有時是無法偵測到它的存在。



Thanos ransomware builder 示意圖

(Source: Recorded Future，https://www.recordedfuture.com/thanos-ransomware-builder)

三、攻擊行為示意圖



當駭客散播惡意軟體 6a50.exe 導致受害主機感染 6a50.exe 後，在主機內會執行 6a50.exe，接著該惡意軟體會進行下面的攻擊行為。

1. 主機會重新開機，並且在開機後進入安全模式。

2. 執行 powershell.exe 來取得 Windows Defender 的資訊並繞過檢測。
3. 執行 net.exe 來停止 36 種防毒軟體的服務程序。
4. 執行 sc.exe 來關閉 4 個非關鍵服務，其中 3 個為與 SQL 有關的服務。
5. 執行 taskkill.exe 來中止 3 個執行中的程序(mspub.exe、mydesktopqos.exe 與 mydesktopservice.exe)。
6. 執行 vssadmin.exe 來刪除所有影子副本與調整陰影複製儲存區關聯的大小上限。
7. 執行 cmd.exe(2572)來清空資源回收桶內所有檔案。
8. 執行 6a50.exe 來加密主機內檔案。
9. 在加密作業完成後，執行 mshta.exe。接著在主機桌面會顯示勒索通知信.hta 檔的視窗訊息。
10. 執行 bcdedit.exe 在開機時取消安全模式。
11. 執行 cmd.exe(3688):

    11.1 將 ping 指令輸出重定向至無效設備。

    11.2 執行 fsutil.exe 來用空資料覆蓋檔案中的資料。

    11.3 在不會跳出提示訊息下強制刪除檔案。
12. 執行 cmd.exe(3708)後呼叫 choice.exe 來在指令時間內進行只有一個 Y 選項的選擇。
13. 刪除惡意軟體 6a50.exe。

四、總結與建議

1. 採用 RaaS(勒索軟體即服務)模式的勒索軟體 Thanos 最早在 2020 年 1 月被發現，並在各種論壇被宣傳與出售，而在 2020 年 7 月初 Thanos 對中東與北非的兩個國有組織進行攻擊。
2. 因 Thanos 的 builder 具有 43 種配置選項，可依照購買者需求自行定義

Thanos 變種樣本，其中包含 RIPlace 技術、繞過防毒軟體偵測、反分析、反 VM 等都是配置選項之一。

3. Thanos 執行後會以安全模式重新啟動受感染的作業系統，從而繞過防毒軟體的檢測。它也會中止 36 種防毒軟體的服務與刪除影子副本。在執行最後 Thanos 會刪除自己本身。
4. 由於 builder 的多功能導致 Thanos 樣本多樣化，容易使防毒軟體未能即時檢測出它，故預防 Thanos 的最佳方法為定期備份資料，不隨意開啟不明來源的檔案或信件。