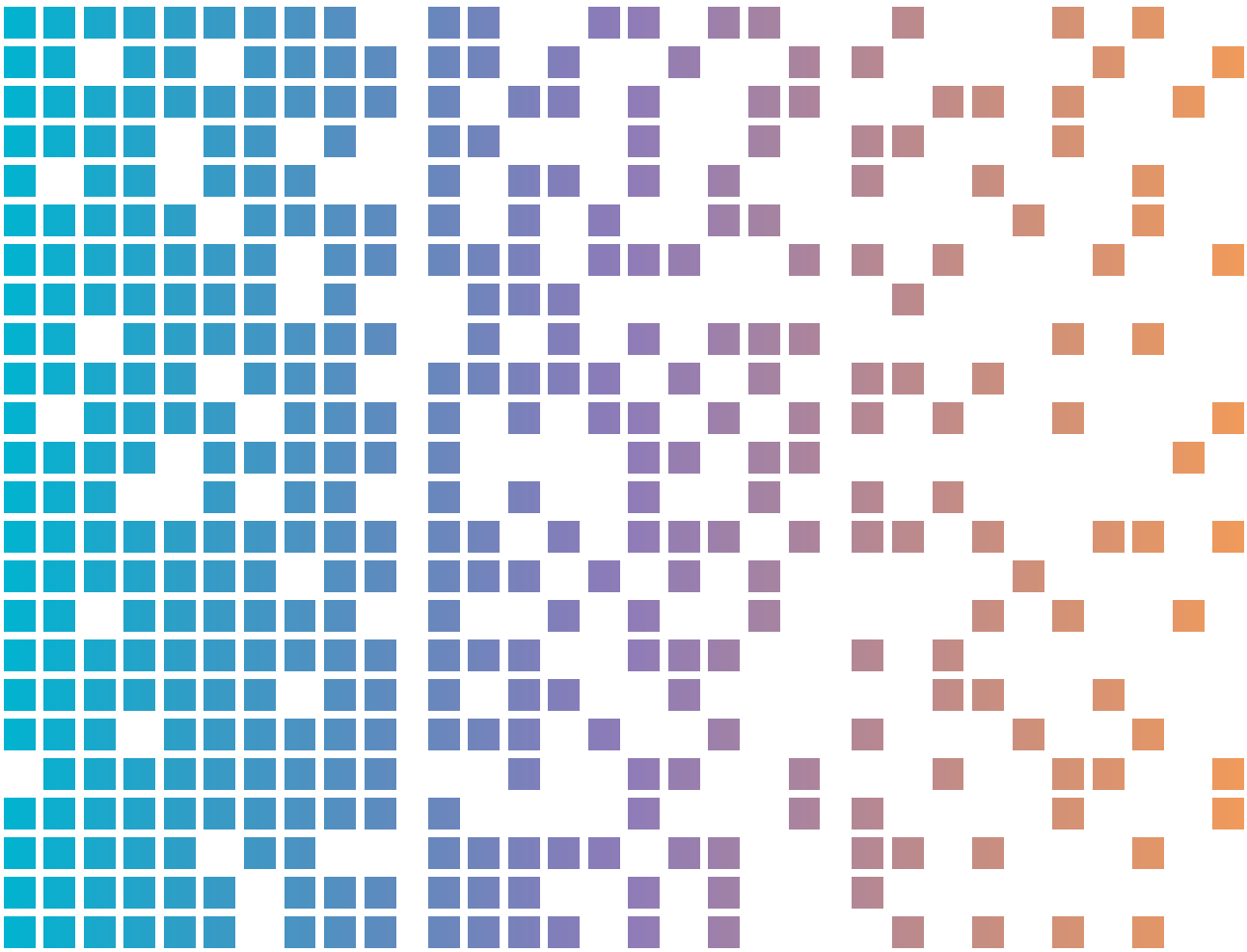
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

無聲盜竊：網絡犯罪分子利用資訊竊取惡意軟件入侵企業網絡



內容複雜程度
中度 ●●○

目錄

現況

資訊竊取惡意軟件 (Information stealer malware) 會盜取使用者憑證和系統資料，讓網絡犯罪分子加以利用，以取得金錢利益。我們在世界球各地（包括澳洲在內）針對不同機構和行業的網絡犯罪攻擊中發現資訊竊取程式踪影。本公告為讀者提供資訊竊取惡意軟件的網絡安全指引，包括為機構及員工提供威脅活動資訊和緩解建議。

重點

- 資訊竊取惡意軟件(Information stealer malware)，也可稱為資訊竊取程式(Info stealers)，是一種設計用來從受害者裝置中收集資料的惡意軟件。包括使用者名稱和密碼、信用卡資料、加密貨幣錢包、本機檔案和瀏覽器資料，包括cookies、使用者歷史記錄和自動填入表單的詳細資料。
- 網絡犯罪分子或會試圖購買和使用與被盜公司帳戶相關的用戶憑證，務求初始入侵受害者的僱主、客戶和其他企業系統。這些機構其後可能會面臨的影響包括勒索軟件、敲詐勒索、商業電子郵件外洩和智識財產權竊盜。
- 澳洲信號局轄下的澳洲網絡安全中心 (ASD 的 ACSC) 留意到企業網絡出現漏洞的原因，是源於員工透過受感染的個人裝置存取工作資料。眾多案例顯示，網絡犯罪分子利用竊取所得的有效使用者憑證，再對公司網絡進行初始入侵。我們的調查顯示，大規模入侵通常是在網絡犯罪分子成功存取特權使用者帳戶後發生的。
- 若機構為員工、承包商、託管服務供應商或其他單位提供可遠端存取的網絡，包括使用自帶設備(BYOD)，便應意識到資訊竊取程式所帶來的風險，並採取措施防範此類威脅。網絡犯罪分子會使用各種技術，將資訊竊取程式部署到受害者的裝置上，包括釣魚電郵、盜版軟件下載、搜尋引擎優化 (SEO) 技術、及廣告或社群媒體平台上發布的惡意連結。一般而言，由於使用者行為及保安控制較少，同時用於工作和個人用途的裝置會有較高風險受易因這些技術而被入侵。
- 資訊竊取程式為網絡犯罪分子提供了一種具吸引力的獲利模式，特別適合入門級或技術能力有限的攻擊者。有些網絡犯罪分子會以惡意軟件即服務 (MaaS) 的形式，推銷資訊竊取產品，並按月收取訂閱費用。

背景

網絡犯罪分子使用資訊竊取程式，對澳洲機構的安全和運作構成威脅。資訊竊取程式感染通常是發生重大網絡安全事故的前奏，因為網絡犯罪分子是利用這類惡意程式收集使用者憑證。這些使用者憑證，特別是有互聯網遠端連結權限或特權帳戶，隨後會被犯罪分子利用對目標公司進行初始入侵以存取系統和資料。

留意：初始入侵經紀在網絡犯罪生態系統中扮演著專門的角色，負責購買和驗證被盜的用戶憑證。隨後，他們會將高質素且具價值的用戶憑證，特別是熱門企業環境的憑證，拍賣予其他網絡犯罪分子，讓買家利用這些憑證入侵該機構的企業網絡。

被盜且有效的使用者憑證對網絡犯罪分子而言極具價值，因為能加快對該企業的網絡和系統進行初始入侵。利用這些竊取所得的有效使用者憑證，網絡犯罪分子可以繞過執行多種典型的策略和技術，包括：

- 識別和研究目標
- 枚舉目標網絡的漏洞
- 開發能作初始入侵的途徑，例如：
  - 製作網絡釣魚資料
  - 利用軟件漏洞
  - 針對遠端服務入侵，包括遠端桌面協定 (RDP) 或虛擬私人網絡 (VPN)
  - 針對使用者憑證暴力破解，如：猜測密碼

執行上述步驟需要投入時間和具備一定的技術能力，對部分網絡犯罪分子來說是一層障礙。特別是對於無法突破公司網絡防禦的網絡犯罪分子而言，資訊竊取程式感染讓他們直接得益，因為感染能提供使用者憑證，讓他們快速、簡單地入侵為目標公司的網絡。

而在遙距工作的環境，部分員工會使用個人裝置，同時進行工作和個人網絡瀏覽。這樣做，員工可能會把使用者憑證儲存在其網頁瀏覽器的密碼儲存和擴充功能中，亦或會使用瀏覽器的自動填入功能。資訊竊取程式的目標包括儲存的密碼，以及網頁瀏覽器中的身份驗證 Cookie 和其他個人資料。

與企業裝置不同，企業安全的策略並未有個人裝置上強制執行，對機構構成更高風險。員工從事如下載盜版軟件或瀏覽高風險網站瀏覽等行為，會增加他們遭受網絡威脅和惡意軟件感染的風險。

在一個以牟利為目標的網絡犯罪生態系統中，構成其核心部分的包括資訊竊取者、分銷商、初始入侵經紀和勒索軟件的相關人士。當網絡犯罪分子專門開發針對某特定階段的能力，然後把該能力作為服務出售給其他犯罪分子時，整個生態系統的效率會有所升。

威脅活動

ASD的ACSC正在追蹤和監察全球資訊竊取活動的增加趨勢，這對澳洲的網絡威脅日益增加。業界報告顯示，資訊竊取程式是 2023 年網絡犯罪活動中最常用的惡意軟件變種。在暗網市場上出售的被盜資料量不斷增加，以及利用這些資料作初始入侵的經紀活動有所增加，反映了此趨勢正在上揚，並於2024年急速發展。

資訊竊取程式的生態系統

第一階段：取得惡意軟件

資訊竊取程式通常在網絡犯罪市場上以MaaS或「惡意軟件即服務」的形式提供，或以原始碼的形式出售。MaaS是一種商業模式，惡意軟件開發人員透過基於網絡平台，向個別人士出售其惡意軟件的訂閱服務，類似合法的「軟件即服務(Saas)」產品。MaaS模式降低了網絡犯罪分子的入門門檻，使缺乏豐富技術的人士也能傳播惡意軟件，並收集竊取所得的資訊以用於網絡攻擊。

以MaaS形式提供的資訊竊取程式通常以相對低廉的月費作招徠，並向網絡犯罪分子提供權限，可利用儀表板管理資訊竊取程式。儀表板用於建立資訊竊取惡意軟件、整理被盜資料，及追蹤受感染系統的數目。 MaaS營運商會提供功能更新、工具和技術支援，以逃避防毒軟件偵測，並吸引和留住訂戶。許多資訊竊取程式更具備自我刪除的功能，能在執行資料外洩後能從受害者的裝置中移除。

第二階段：散佈

傳播資訊竊取程式及從受感染裝置收集資訊的網絡犯罪分子被稱為網絡流量販子(Traffer)。作為計劃的一部分，網絡流量販子會引導受害者點擊惡意連結，協助傳播資訊竊取程式，大多數計劃都是無差別的，感染與否全視乎機會。但是，也有計劃是針對特定行業或特定受害者而定的魚叉式網絡釣魚。網絡流量販子會根據客戶需求，執行這些具針對性的計劃；例如，買家尋求入侵特定被視為高價值目標的機構或部門。

網絡流量販子會運用多種技術將資訊竊取程式部署到受害者設備上，包括：

- **殭屍網絡**：由網絡犯罪者控制的受感染電腦系統網絡，以執行惡意操作，例如發送網絡釣魚訊息或惡意軟件

- **網絡釣魚**：試圖透過欺騙手段獲取敏感資訊，包括透過電郵，或在社交媒體、論壇和通訊應用程式上的直接訊息。這些常見的傳播方式降低了網絡犯罪者的入侵門檻：
  - 這些訊息通常含有惡意連鏈，而非直接在電郵裡附加惡意檔案
- **惡意搜尋結果**：透過搜尋引擎優化 (SEO) 技術，將目標引導至偽裝成合法軟件或其他內容的惡意軟件網站
- **惡意廣告**：將有害的程式碼加進合法的網絡廣告中，以圖傳播惡意軟件
- **破解或盜版軟件**：透過YouTube影片分享的下載內容（包括遊戲）、影片說明或評論中含有惡意連結，或來自不可信的下載網站
- **社交媒體廣告與貼文**：將目標對象引導至偽裝的惡意軟件檔案
- **惡意軟件更新**：通常會偽裝成網頁瀏覽器的更新檔

第三階段：資料收集

一旦資訊竊取程式在受害者的設備上執行，便會開始從受感染的裝置中收集敏感資料。除竊取使用者憑證外，如果資訊竊取者是殭屍網絡的一部分，網絡犯罪分子還可以發送設定指令，以啟動其他功能或傳播其他惡意軟件，從遠端控制受感染的裝置。一般來說，資訊竊取者能夠竊取：

- 使用者名稱和密碼，特別是儲存在 Web 瀏覽器的多因素身份驗證 (MFA) 使用者工作階段/權杖。
- 身份驗證 Cookie
- 網頁瀏覽器的表單自動填入訊息
- 電郵憑證、內容和聯絡人
- 網頁瀏覽紀錄
- 使用者檔案
- 信用卡詳細信息
- 桌面訊息應用程式的聊天記錄
- 系統資訊
- 加密貨幣錢包
- VPN 或檔案傳輸協定 (FTP) 憑證

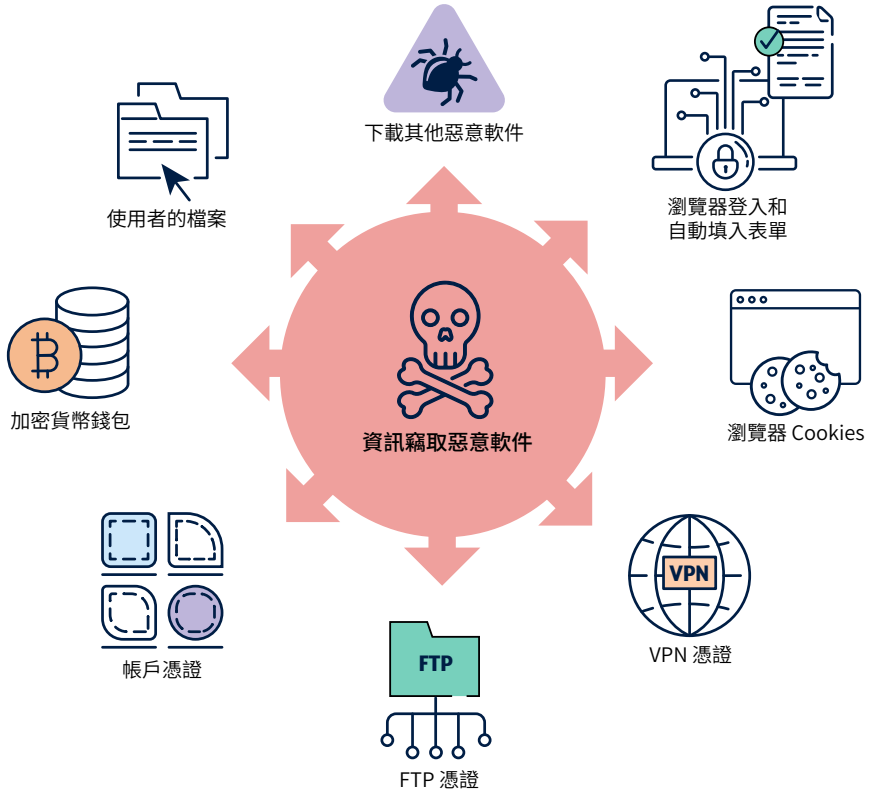


圖1: 資訊竊取程式的功能

有些網頁瀏覽器驗證cookie會讓使用者一次登入帳戶或服務多日，令使用者就不需要重新進行身分驗證。如果被盜，這些身分驗證cookie可以有效繞過MFA 要求，並為網絡犯罪分子提供進入受害者帳戶、公司網絡和企業系統的權限。

第四階段：資料整合與獲取利益

資訊竊取程式會將受害者資訊（稱為「日誌log」）洩漏到惡意軟件的命令和控制伺服器。一般來說，資訊竊取者利用流行的即時訊息應用程式（例如Telegram和Discord）以向網絡犯罪分子共享日誌內容。

Telegram 和暗網上設有專門的交易市場，以銷售和交易日誌。網絡犯罪分子能利用多種途徑透過日誌獲利，包括：

- 在犯罪市場上出售日誌，包括售予初始訪問經紀。
- 透過身分盜竊和勒索手法，直接對受害者造成傷害。
- 利用這些資訊對公司網絡進行初始入侵和勒索軟件活動。

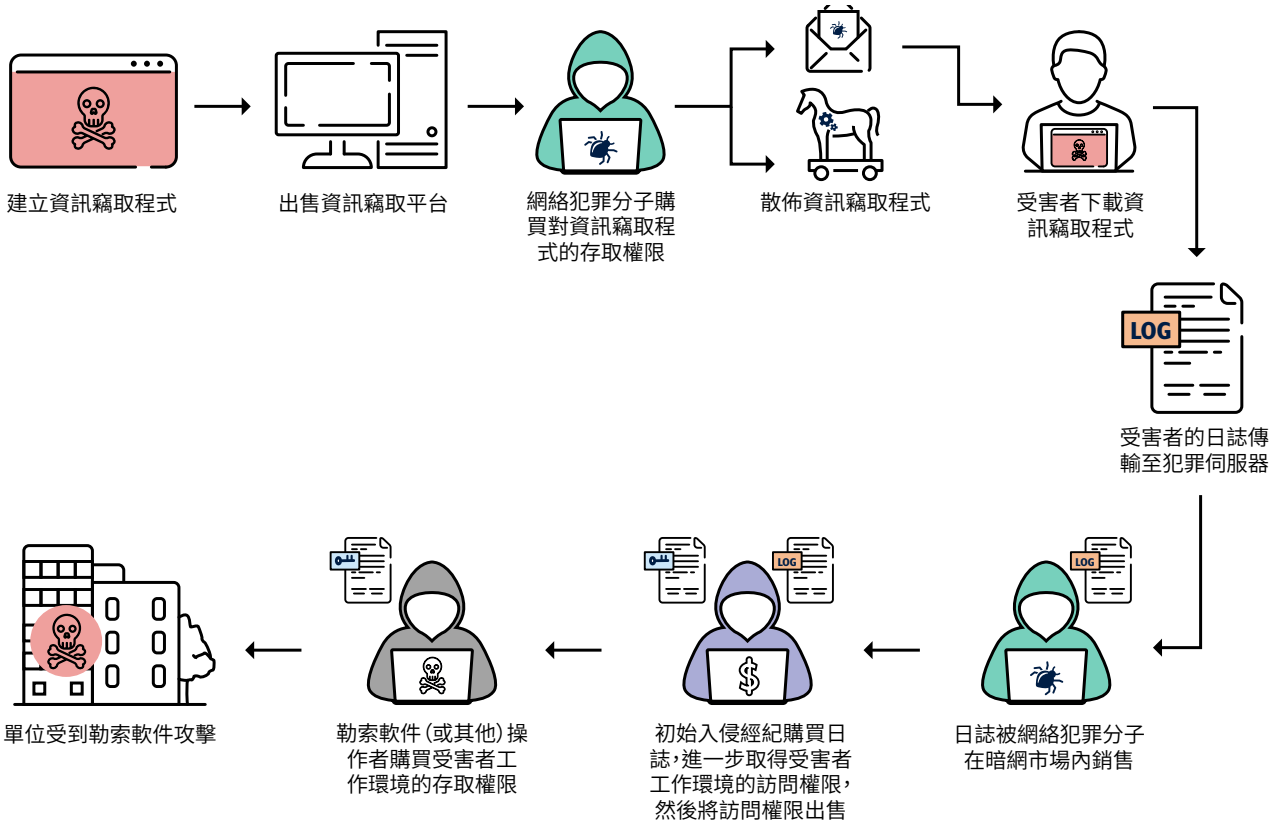


圖2: 資訊竊取程式的生態系統及其對機構的可能影響

影響

資訊竊取程式或會對個人和機構造成嚴重影響。當資訊竊取程式收集到使用者憑證後，網絡犯罪分子可利用這些使用者憑證，利用有效的使用者帳戶，以存取公司網絡或企業系統，並導致系統管理員延遲偵測到異常。

若**機構**受到資訊竊取程式所影響，後果可能包括：

- 勒索軟件
- 資料外洩
- 企業電郵入侵
- 智識財產權被竊
- 敏感資訊被竊。

對於受到資訊竊取程式影響的**人士**，後果可能包括：

- 個人電郵或社交媒體帳戶被未經授權存取
- 增加身份盜竊風險
- 增加網絡釣魚攻擊的風險
- 金錢損失或財務帳戶被未經授權存取
- 隱私被侵犯。

個案分析

本個案研究的內容已作匿名處理，以作公開發佈之用。綜合了多個影響澳洲機構且已向澳洲安全情報組織（ASD）的澳洲網路安全中心（ACSC）報告的網路安全事件。受影響的單位以下稱為「該機構」。本個案研究中的個人姓名均為虛構，為保護受害者身份，詳細資料已被刪除。

該機構是一家澳洲企業，允許員工透過個人裝置存取公司系統。愛麗絲是該機構的員工，能遠距離工作。

在家工作時，愛麗絲使用她的個人手提電腦，透過遠端存取進入機構的企業網絡。愛麗絲從她認為是合法的網站上**下載**了Notepad++（一種筆記軟件）的一個版本到她的**個人筆記簿型電腦**上，而這其實是一個偽裝成Notepad++安裝程式的**資訊竊取程式**。

當愛麗絲嘗試安裝軟件時，資訊竊取程式就被啟動並開始從她的手提電腦**收集使用者憑證**。當中包括她保存在網頁瀏覽器的已儲存登入功能，用於工作的使用者名稱和密碼。資訊竊取程式及後將這些使用者憑證傳送到由網絡犯罪集團操控的遠端命令和控制伺服器。

被竊取的記錄與其他資料一併打包，並透過**暗網市場出售予網絡罪犯**。

一個叫鮑伯的網絡罪犯購買了愛麗絲的使用者憑證，該憑證涵蓋她所在機構網絡中多項服務的身份認證資料。愛麗絲的機構**沒有為服務設定MFA功能**，這代表鮑伯可以僅憑被盜的使用者憑證，就可成功**驗證身分並存取**公司網絡。

鮑伯使用被盜的**有效使用者憑證**，在未被發現的情況下存取了該機構的企業網絡。鮑伯成功在公司網絡中橫向移動，識別出屬於該機構的敏感資料，並將其非法外洩以勒索公司。

竊取敏感資料後，鮑伯將該機構的**資料庫和檔案系統加密**，導致其無法存取。

緩解措施

機構可能無法對連接到公司網絡的裝置實施控制，尤其是員工在遠端工作時使用的個人裝置。澳洲信號局轄下的網絡安全中心建議各機構專注實施控制措施，以減低受資訊竊取程式針對盜取使用者憑證所帶來的風險。緩解措施包括：

為員工提供網絡安全意識培訓

- 透過向員工提供有效的培訓，防止針對性的社交工程攻擊及惡意檔案下載得逞。
- 提高機構對資訊竊取程式、其傳播方式，以及網絡釣魚威脅之認識與警覺。

保護公司帳戶安全

- 實施多重身份驗證 (MFA)：
- 應實施多重身份驗證（MFA）於所有外部及內部服務、系統，以及敏感資料儲存庫中，特別是網絡電郵、虛擬私人網絡（VPN）和存取關鍵系統的特權帳戶。最佳做法是於所有帳戶上實施防護網絡釣魚的MFA。
- 停用不再需要的使用者帳戶。
- 限制管理員權限：
- 僅使用專用而受限的工作站（如安全的管理員工作站）以執行網絡管理和其他特權操作。
- 根據最小權限原則的最佳實踐，管理員只在進行系統管理才使用有特權使用者帳戶。在處理非管理相關的日常工作時，應使用標準使用者帳戶。
- 防止特權使用者帳戶存取網際網絡、電子郵件和網絡服務，但獲得明確授權存取網上服務的帳戶除外。
- 考慮對系統和應用程式實施按需授權管理。
- 加強對特權使用者帳號的管理和稽核。
- 定期更新密碼，尤其是面向外部連線的遠端存取帳戶。
- 強制實施對工作階段權仗和Cookie的有效期限逾時和日落策略。

強化企業流動性安全

- 進行企業流動性的風險評估，並實施企業流動性強化指南。
- 如允許員工使用個人設備處理工作事務，應制定自攜設備 (BYOD) 政策，因公司管理的裝置較未受管理的個人裝置安全。

審視及評估供應鏈風險，特別是能存取貴機構網絡的供應商，包括軟件即服務(SaaS)供應商及託管服務供應商。在聘用託管服務供應商時應如何管理您的資訊安全。

保護您的企業網絡

- 保持應用程式和作業系統為最新版本。
- 套用本機安全性策略，並透過嚴格的允許清單以實施應用程式控制。
- 實施網絡分段，根據職位角色和功能，把網絡劃分為不同區段。
- 稽核及監察用戶活動，特別是遙距工作的員工。
- 對高權限帳戶的活動監察，有助偵測未經授權存取敏感資料的行為，或異常的數據傳輸活動，例如大量數據被上傳至外部網絡。
- 實施資料外洩防護政策及相關工具，以防止未經授權的資料傳輸。

成為ASD網絡安全網絡合作夥伴，並加入ASD的網絡威脅情報共享(CTIS)服務

- CTIS是一個雙向共享平台，使政府和業界的合作夥伴能夠接收和分享有關惡意網絡活動的資訊。
- ASD的ACSC正在追蹤資訊竊取活動，並透過CTIS平台分享主動指揮和控制基礎設施。
- 註冊成為合作夥伴，以保護您的機構和客戶資料免受網絡犯罪威脅。

做好被入侵的準備

- 制定網絡安全事故的應變計劃，以應對資訊竊取程式入侵引致的事件。確保員工清楚知道，懷疑下載可疑檔案後他們應採取的行動及聯絡對象。

執行 ASD 的 ACSC 八項基本原則

- 除了上述的緩解措施外，ASD的ACSC 強烈建議實施 ASD 的 ACSC 八項基本措施 (Essential Eight) 的其餘部分。

為遙距工作的員工提供建議

- 保護您個人裝置上的資料
  - 養成良好的網絡衛生習慣，不要點擊可疑連結或彈出視窗，也要從未知或不受信任的來源下載檔案或軟件。
  - 不為工作和個人帳戶設定不同的密碼。於可行的情況下，套用MFA至個人帳戶的使用。
  - 除非得到僱主的明確批准，否則請勿將您的工作憑證儲存在個人的密碼管理員，這包括在網頁瀏覽器內的密碼管理員。**如有疑問，請要求您的僱主提供獲公司支援的密碼管理員。**
  - 不要從共用或公共的工作電腦登入您的工作帳戶。
  - 要注意網頁瀏覽器的自動填入功能中儲存了什麼資料。資訊竊取程式會針對瀏覽器用作自動填表所儲存的資料。在填寫網頁表單時，應考慮手動輸入敏感資料（例如信用卡號碼），而非儲存在瀏覽器的自動填入功能中。
  - 瀏覽結束後，請登出所有網上服務並清除網頁瀏覽器Cookie，以減少資訊竊取程式可盜取的資訊。
  - 確保已啟用作業系統內建的防毒功能。如果使用第三方防毒解決方案，應確保是來自信譽良好的供應商，並保持更新至最新版本。

協助

受資訊竊取程式入侵影響或需要協助的澳洲機構，可致電 **1300 CYBER1 (1300 292 371)** 聯絡 ASD 的 ACSC，或在 cyber.gov.au/report 提交報告。

ASD 的 ACSC 鼓勵各機構，即使事件已受控制，亦應通報可疑的網絡活動，及提供資訊竊取程式的相關入侵指標。您所提供的資訊，將有助我們加深了解網絡入侵的戰術、技術及程序，從而協助我們警告其他遭受同類攻擊的澳洲機構。

如需了解詳情或通報網絡安全事件，請聯繫我們：

cyber.gov.au | 1300 CYBER1 (1300 292 371)

此號碼僅適用於澳洲境內。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre