APT40 公告

中國國安部近期行動所用的技術

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

目錄

近況 5

背景 5

活動摘要 5

值得留意的技術 6

工具 7

個案研究 7

個案研究(一) 8

執行摘要 8

調查結果 9

詳情 9

視覺時間線 9

詳細時間線 10

攻擊者的戰術與技術 11

偵察 11

初始入侵 11

執行 11

存取憑證 11

橫向移動 11

收集資料 11

資料外傳 11

個案研究(二) 12

執行摘要 12

調查結果 13
調查摘要 13
內部主機 13
調查時間線 14
攻擊者的戰術與技術 11
初始入侵 15
執行 15
持久性 15
權限提升 15
存取憑證 15
偵察 16
收集資料 16
指揮與控制 16
偵測與緩解建議 17
偵測 17
緩解措施 20
MITRE ATT&CK – APT40 曾使用且值得關注的攻擊技術 22

概述

背景

本公告由下列機構撰寫：包括澳洲信號局轄下的澳洲網絡安全中心、美國網絡安全及基礎設施安全局、美國國家安全局、美國聯邦調查局、英國國家網絡安全中心、紐西蘭政府通訊安全局轄下的紐西蘭國家網絡安全中心、德國聯邦情報局、德國聯邦憲法保衛局、大韓民國國家情報院及轄下的國家網絡安全中心，和日本內閣網絡安全戰略本部及日本警察廳。及後文件內會統稱為「撰寫機構」。本公告概述中華人民共和國政府支持的網絡組織，以及他們對澳洲網絡的目前威脅。本公告是根據各撰寫機構對有關威脅的共同理解，及澳洲訊號局轄下網絡安全中心（ASD 的 ACSC）進行的事件回應調查所得資料編製而成。

中國政府支持的網絡攻擊組織曾針多個國家的機構發動攻擊，包括澳洲及美國，下文所述的技術均為中國政府支持的網絡攻擊者常用手法。故此，撰寫機構認為該組織及其類似技術，仍對各撰寫國家的網絡構成威脅。

撰寫機構評估該組織是為中華人民共和國國家安全部（MSS）執行惡意網絡活動。有關組織的活動和技術，與被追蹤的進階持續性威脅（APT）40（業界報告也稱其為 Kryptonite Panda、GINGHAM TYPHOON、Leviathan 和 Bronze Mohawk）的組織有所重疊。據報該組織過往據點位於中國海南省海口市，進行受中國國家安全部海南省國家安全廳所指派任務。[2] 本公告隨後提供了此對手針對兩個受害網絡時，所採用技術的若干重要個案研究。這些個案研究對於網路安全從業人員具有重大意義，有助於其識別、預防並修復APT40對自身網路的入侵行為。所選的個案研究均已採取適當補救措施，以減低這些威脅行為者或其他攻擊者再次利用相同漏洞的風險。所以，個案研究通常是較早前發生的，確保機構有足夠的時間進行補救。

活動摘要

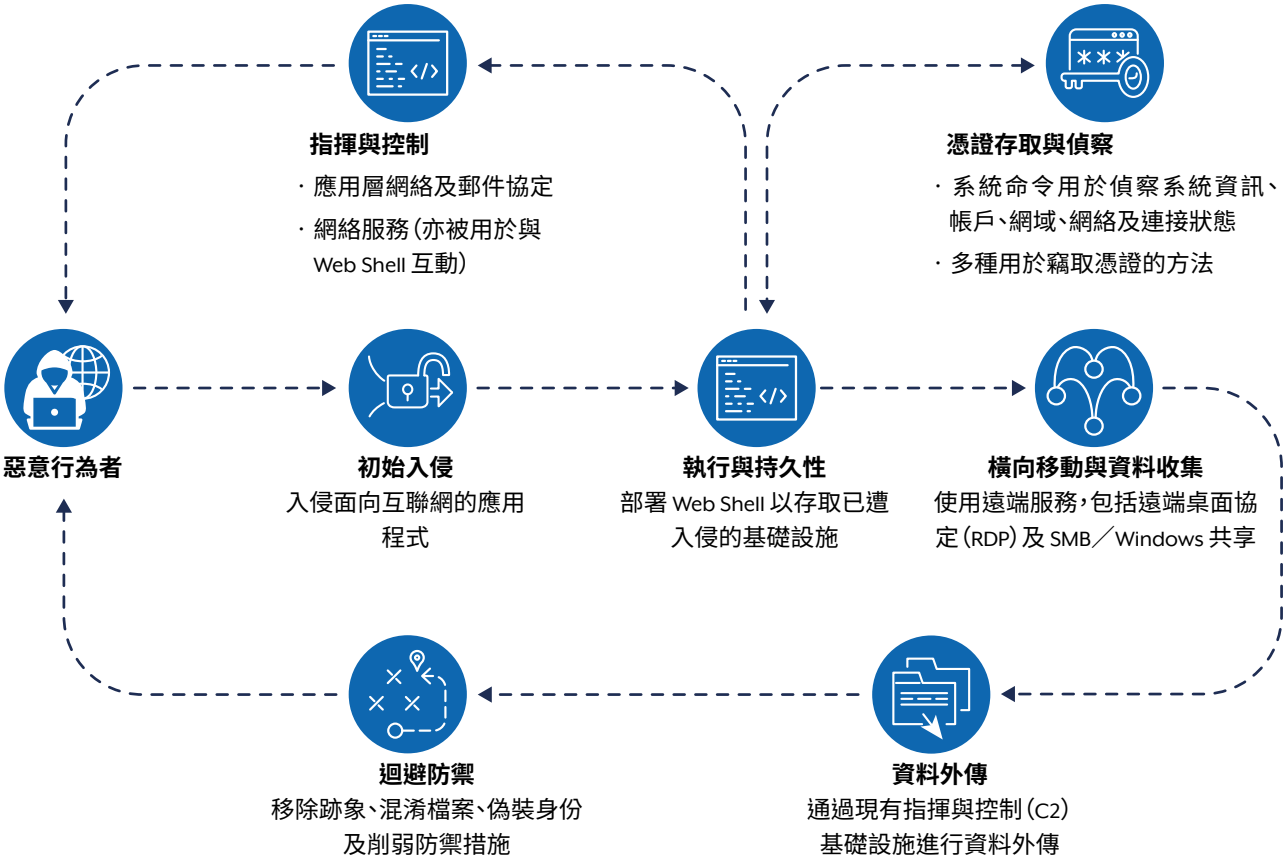
APT40 多次針對澳洲的網絡，及政府和私營機構的網絡作出攻擊，持續威脅著我們網絡。本公告中所描述的技術經常出現在針對澳洲網絡的攻擊中。

值得注意的是，APT40 具備能力能快速改造及應用新發現漏洞的概念性攻擊程式碼（PoC），並能即時針對受有關漏洞影響的目標網絡，對其基礎設施發動攻擊。APT40 定期對其感興趣的網絡進行偵察，包括撰寫機構所在國家的網絡，尋找入侵目標的機會。透過定期偵察，組織可以識別目標網路中存在漏洞、停止支援或不再受維護的裝置，並快速部署攻擊。APT40 自 2017 年起就持續利用漏洞成功入侵。

APT40 迅速利用常用軟件中剛公開的漏洞發動攻擊，例如 Log4J (CVE 2021 44228)、Atlassian Confluence (CVE-2021-31207、CVE-2021-26084、(CVE-2021-31207; CVE-2021-34523; CVE-2021-34473)。ASD 的 ACSC 和撰寫機構相信，該組織會在漏洞公開發布後的數小時或數天內，持續使用 POC 來入侵備受關注的漏洞。

2 美國司法部. 2021. 四名與中國國家安全部合作的中國公民，被控在全球進行電腦入侵活動，目標是知識產權和商業機密，包括傳染病研究。

圖 1: APT40 活動的戰術、技術及程序 (TTP) 流程圖



該組織似乎更喜歡利用易受攻擊的、面向公眾的基礎裝置,而非依賴需要與使用者互動的技術 (例如網絡釣魚),並且高度重視獲取有效憑證,以進行一系列的後續活動。APT40 經常使用 Web Shell (T1505.003) 以求取得持久性,特別是在入侵的初期。通常在成功初始入侵後,APT40 會專注於建立持久性,以維持對受害者系統環境的持續存取權限。然而,由於持久性滲透行為在入侵的早期就已出現,因此無論入侵程度或後續行動如何,都較有可能在所有入侵事件中被觀察到。

值得關注的攻擊技術手法

儘管 APT40 過往曾利用遭入侵的澳洲網站作為其行動的指揮與控制 (C2) 主機,但該組織的相關技術已有演變 (T1594)。

APT40 跟隨全球趨勢,使用受感染裝置 (包括小型辦公室/家庭辦公室 (SOHO) 裝置) 作為其在澳洲開展行動的營運基礎設施,和最後一跳時的重定向器(T1584.008)。這讓撰寫機構能更有效地描述和追蹤該組織的動向。

許多 SOHO 裝置的產品支援已終止或未有安全更新,成為利用 N-day 漏洞攻擊的高風險目標。一旦遭到入侵,SOHO 裝置就會成為攻擊的起點。這些攻擊旨在融入合法的流量,並挑戰網絡防禦 (T1001.003)。

這種技術也經常被世界各地其他受中國政府支持的人士使用,而撰寫機構認為這是一種共同的威脅。若需更多資料,請參閱下列聯合公告:中華人民共和國國家支持的網絡行為者利用網絡提供商和裝置和中華人民共和國國家支持的行為者入侵並持續存取美國關鍵基礎設施。

APT40 確實偶爾會在其行動中使用採購或租賃的基礎設施,作為面向受害者的指揮與控制 (C2) 基礎設施,惟有關技術手法近年似乎相對減少使用。

工具

ASD的ACSC正公開分享在以下調查中識別所知的一些惡意檔案。這些文件已上載至 VirusTotal，讓更廣泛的網絡防禦和網絡安全社群進一步了解他們需要防禦的威脅。

個案研究

ASD 的 ACSC 正公開分享兩份經匿名處理的調查報告，以提高人們對犯罪分子如何使用其工具和技巧的認識。

MD5	檔案名稱	更多資訊
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

個案研究（一）

本報告已經匿名化處理，以便廣泛傳播。受影響機構於下文中統稱為「該機構」。部分具體細節亦經刪除，以保障受害者身份及ASD的ACSC對事件的回應方法。

執行摘要

本報告詳細介紹了ASD的ACSC對2022年7月至9月期間，該機構網絡被成功入侵事件的調查結果。調查報告已提供予該機構，總結觀察到的惡意活動並提供補救建議。調查結果顯示此次入侵是 APT40 所為。

在8 月中旬，ASD的ACSC通知該機構，其網絡在八月下旬遭遇來自疑似被該組織入侵裝置的惡意互動。經獲該機構同意後，ASD的ACSC隨即在該網絡中可能受影響的主機部署了主機端感測器，讓ASD的ACSC的事件應對分析員能全面地進行的數碼鑑證調查。利用感測器的所得數據，ASD的ACSC分析員成功繪製了該組織的活動圖，並製作了觀察到的事件的詳細時間表。

從7月到8月，ASD的ACSC觀察所得的主要攻擊者活動包括：

- 主機枚舉，令攻擊者能建立其網絡地圖；
- 使用 Web Shell，讓攻擊者在網絡中獲得初步立足點及執行指令的能力；
- 部署其他攻擊工具，以達致惡意目的。

調查發現了大量敏感資料被存取的證據，以及攻擊者在網絡中橫向移動的證據 (T1021.002)。大部分的入侵活動之所以能夠得逞，主要是由於攻擊者在目標網絡中建立了多個存取向量、扁平的網絡結構，以及使用了由內部開發、能被用作隨意上傳檔案的不安全軟件。被外傳的資料包括特權憑證，使攻擊者能夠登入系統，以及網絡資訊，讓攻擊者在原始存取向量遭封鎖後，在未經授權下能重新取得的存取權限。除了初始入侵時用到的惡意程式，未有發現其他的惡意工具；然而，該組織若能掌握合法及具特權的身份驗證憑證，便無需額外的工具即可執行各種行動。調查結果表明，該機構很可能是 APT40 故意針對的，而不是因為眾所周知的漏洞而遭到攻擊。

調查結果

在2022年8月中旬，ASD的ACSC通知該機構，一個已確認的惡意IP（據信與國家支持的網絡組織有關）曾在7月至8月期間與該機構的電腦網絡進行過互動。被入侵的裝置可能屬於小型企或家庭用戶。

在8月下旬，ASD的ACSC向機構的網絡主機部署一個基於主機的代理程式，顯示出受到攻擊影響的跡象。

由於日誌配置或網絡設計的限制，導致部份本來可以支援調查工作的資料無法被利用。儘管如此，因為該機構準備提供所有可用數據，使ASD 的 ACSC事件反應人員能夠進行全面分析，有助掌握可能是APT40在網絡上的活動。

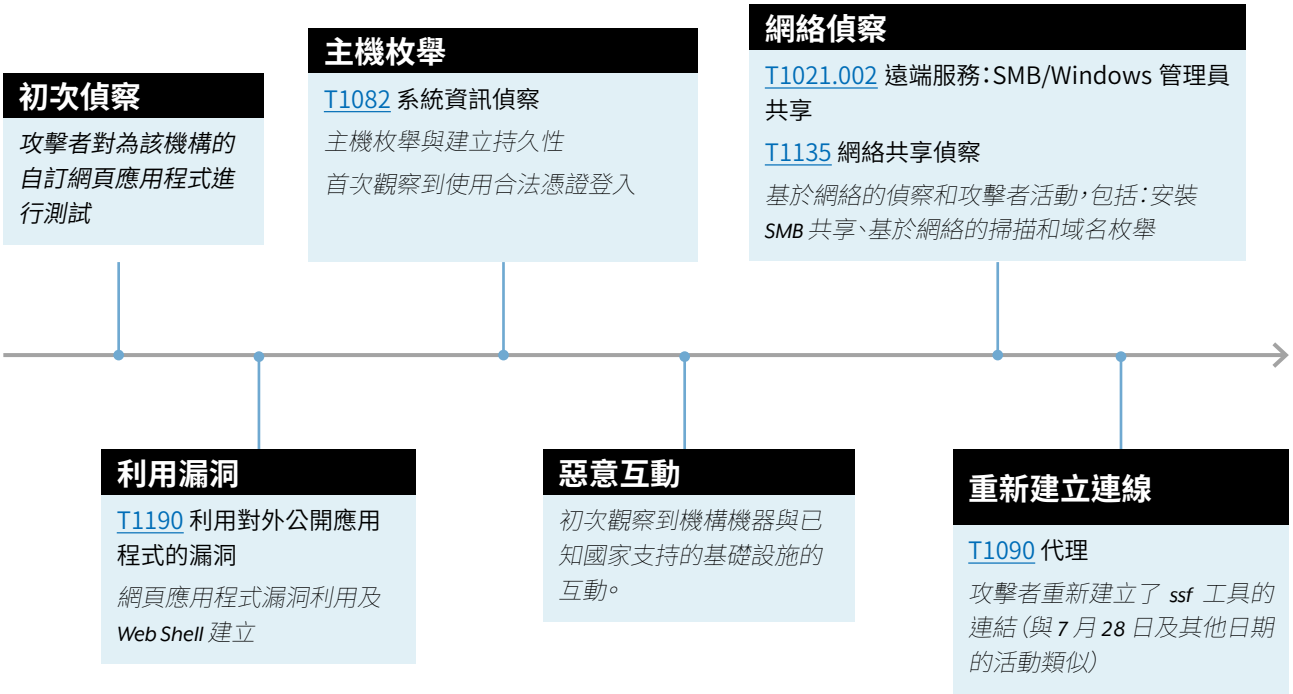
在9 月，經過與ASD的ACSC協商後，該機構決定將最初通報中提及的IP地址列入拒絕名單，並在10月開始採取補救措施。

詳細資訊

從 7 月開始，攻擊者能夠成功測試並利用運行於`<webapp>2-ext` 的自訂Web 應用程式 (T1190)，令該組織能夠在網絡隔離區 (DMZ) 建立據點。這據點被用來枚舉網絡以及所有可見的網域名稱。被盜用的憑證 (T1078.002) 被用於查詢 Active Directory (T1018)，並透過掛載多台位於 DMZ 內的機器的檔案共享 (T1039) 來外洩資料。攻擊者曾發動Kerberoasting攻擊，以便從伺服器 (T1558.003) 取得有效的網絡憑證。該組織並未觀察到在DMZ或內部網絡中獲得任何額外的活動據點。

視覺時間表

以下時間表概述了於該機構網絡上所觀察到的惡意行為者活動的主要階段。



詳細時間表

7月：攻擊者初次初始連線，連往一項自訂Web應用程式的首頁(T1190)，此程式是該機構自行編寫的(以下稱為「Web 應用程式」或「*webapp*}」)，連線是透過傳輸層安全性 (TLS) 連接 (T1102)。未觀察到其他值得注意的活動。

7月：攻擊者開始枚舉該 Web 應用程式的網站，尋找端點[2] 以便進一步調查。

7月：攻擊者集中於嘗試利用特定端點進行攻擊。

7月：攻擊者成功透過另一頁面植入的 Web Shell，以 `POST` 方式向網絡伺服器發送請求。另一個 IP 地址，可能是由同一攻擊者使用，也開始向相同的URL發送請求。攻擊者建立並測試了多個疑似 Web Shell。

雖然具體的利用方法不明，但可以確定該特定端點被鎖定以在 *<webapp>2*-ext 創建檔案。

ASD的ACSC認為，這兩個 IP 位址連線屬於同一次入侵，原因是它們具有共同目標，而且初始連線時間相隔僅幾分鐘。

7月：該組織繼續進行主機枚舉，尋找提升權限的機會，並部署不同的 Web Shell。攻擊者使用被盜取的憑證來登入該網頁應用程式，憑證格式為*<firstname.surname>@<organisation domain>*。

攻擊者的活動似乎未能成功在 *<webapp>2*-ext 上提升權限。相反地，攻擊者轉向進行基於網絡的活動。

7月：攻擊者測試被盜用的服務帳戶憑證[3]，該憑證很可能是從內部可存取的二進位檔中硬編碼取得的。

7月：攻擊者部署了開源工具Secure Socket Funnelling，用以連接至惡意基礎設施。該連接被用來將流量從攻擊者的攻擊機器傳輸到機構的內部網絡，當他們嘗試使用服務帳戶憑證時，機器名稱便會曝露在事件日誌中。

8月：觀察顯示攻擊者的活動不多，包括未能成功建立與服務帳戶相關的連線。

8月：攻擊者執行一定數量的網絡及Active Directory枚舉活動。隨後，另一個被入侵的帳戶被用於在DMZ內的Windows機器上掛載共享資源[4]，令資料外洩能得以成功。

這似乎是利用DMZ中可掛載機器所進行的機會式憑證濫用行為。防火牆阻止了攻擊者針對內部網絡進行類似活動。

8月至9月：SSF工具重新建立了與惡意IP位置的連線。該組織並未觀察到有任何其他活動，直至其存取權被封鎖。

9月：該機構透過在防火牆上將惡意 IP 地址加入拒絕名單來阻擋其連線。

2 在這個案中，端點指的是 Web 應用程式的一項功能。

3 服務帳號並非與個人使用者綁定，而是與服務綁定。在 Microsoft 企業網域中，存在多種類型的帳戶。

4 掛載共享是指將檔案系統結構中的檔案，開放給使用者或使用者群組存取的過程。

攻擊者的戰術與技術

MITRE ATT&CK框架是一套記錄網路威脅行為者在網絡空間所採用戰術與技術的資料庫。此框架由美國非營利組織 MITRE公司創建，作為描述威脅行為者行為的全球通用語言。

ASD的ACSC評估下列技術和戰術，與攻擊者的惡意活動相關：

偵察

T1594 – 搜尋受害者擁有的網站

攻擊者對自訂Web應用程式的網站進行枚舉，以尋找存取網絡的機會。

初始入侵

T1190 利用面向公眾的應用程式（關於入侵自訂的 Web 應用程式）

T1078.002 – 有效帳戶：網域帳戶（關於利用被洩漏的憑證登入）

攻擊者利用對外公開的自訂Web應用程式作為初始存取點。及後使用已洩漏的憑證，進一步擴展對網絡的存取權限。

執行

T1059 – 指令與腳本解譯器（關於透過Web Shell執行指令）

T1072 – 軟件部署工具（關於攻擊者使用開源工具Secure Socket Funnelling（SSF）連接至某 IP）

持久性

T1505.003 – 伺服器軟件組件：Web Shell（關於使用 Web Shell 和 SSF 建立存取權限）

存取憑證

T1552.001 – 密碼儲存中的憑證（關於與樓宇管理系統（BMS）相關的密碼檔案）

T1558.003 – 竊取或偽造 Kerberos 票證：Kerberoasting（關於獲取網絡憑證的攻擊）

橫向移動

T1021.002 – 遠端服務：SMB 共用（關於攻擊者從多個裝置安裝 SMB 共用分享）

收集

T1213 – 來自資訊儲存庫的資料（關於 BMS 伺服器上的手冊/文件）

資料外傳

T1041 – 透過C2通道進行資料外洩（關於攻擊者從 Active Directory 洩漏資料並掛載共用）

個案研究(二)

本報告已經匿名化處理,以便廣泛傳播。受影響機構於下文中統稱為「該機構」。部分具體細節已經刪除,以保障受害者身份及ASD的ACSC對事件的回應方法。

執行摘要

本報告詳細介紹了ASD的ACSC在2022年4月,該機構網絡被成功入侵事件的調查結果。調查報告已提供予該機構,總結觀察到的惡意活動並提供補救建議。調查結果顯示此次入侵是APT40所為。

2022年5月,ASD的ACSC通知某機構,其網絡自2022年4月起懷疑存有惡意活動。隨後,該機構通知ASD的ACSC,他們在面向互聯網的伺服器上發現了惡意軟件,該伺服器是為機構的企業遠端存取方案提供登入入口。此伺服器使用一款遠端存取登入和身分管理產品,於本報告中稱之為「受感染裝置」。本報告詳列ASD的ACSC的調查結果,以及為該機構制訂的補救建議。

有證據顯示,自2022年4月開始,機構網絡的一部份已透過其遠端存取登入入口遭到惡意網絡行為者入侵。該伺服器可能曾遭多方攻擊者入侵,並很可能受到入侵時廣泛披露的遠端程式碼執行(RCE)漏洞所影響。

ASD的ACSC觀察所得的主要攻擊者活動包括:

- 主機枚舉,令攻擊者能建立其網絡地圖;
- 入侵面向互聯網的應用程式和使用Web Shell,讓攻擊者在網絡中獲得初步立足點及執行指令的能力;
- 利用軟件漏洞以提升權限;以及
- 收集憑證以進行橫向移動

ASD的ACSC發現,一名惡意行為者於2022年4月在受感染的裝置上洩露了數百組獨特的使用者名稱和密碼,以及多組與遠端存取工具階段相關的多重身分驗證程式碼和技術資料。經該機構審查後,確認這些密碼屬於真實有效的帳戶憑證。ASD的ACSC評估認為,攻擊者可能收集了這些技術資料,以劫持或冒充合法使用者建立遠端登入工作階段,並透過合法帳戶以存取機構的內部企業網絡。

調查結果

調查摘要

ASD的ACSC確定，攻擊者入侵了為機構員工提供遠端登入工作階段的裝置，並以此入侵嘗試進行後續活動。這些裝置由三台負載平衡的主機組成，最早的入侵證據就是在這些主機上被偵測到。初始入侵後不久，該機構就關閉了三台負載平衡主機中的其中兩台。因此，後續的所有活動都集中在單一主機上。與受入侵裝置相關的其他伺服器亦是採用類似的負載平衡方式。為便於閱讀，本報告的大部分內容會將所有受入侵的裝置稱為「單一裝置」。

據信該攻擊者自2022年4月起，利用公開已知的漏洞，將 Web Shell 部署到受入侵的裝置上。評估顯示，該組織的威脅行動者已在裝置上取得提升了的權限。由於缺乏可用的日誌記錄，ASD的ACSC無法確定該入侵活動的全部範圍。然而，裝置上的證據表明，攻擊者已成功執行以下活動：

- 收集數百對真實的使用者名稱和密碼；及
- 收集的技術資料可能讓惡意行為者能以合法使用者身分，存取虛擬桌面基礎架構（VDI）工作階段。

ASD的ACSC評估該攻擊者會試圖進一步入侵該機構的網絡。攻擊者竊取的資料可能使他們能以合法使用者的身份（根據他們的選擇，包括管理員）劫持或啟動虛擬桌面工作階段。攻擊者可能已經利用此存取向量，進一步破壞機構的服務，以實現持久性和其他目標。

在託管服務提供商管理環境內的其他機構裝置，並沒有顯示遭受入侵的跡象。

存取

受入侵裝置的主機透過Active Directory和Web伺服器，為連接到VDI 工作階段的使用者提供驗證服務 (T1021.001)。

位置	受入侵裝置的主機名稱（負載平衡）
資料中心 1	HOST1, HOST2, HOST3

該裝置基礎設施亦包括存取閘道主機，一旦使用者擁有從裝置產生和下載的身份驗證權杖，該主機就會為使用者提供 VDI的通道。

無任何證據顯示這些主機受到入侵。然而，存取閘道主機的日誌顯示，有證據與已知惡意IP位址存在大量互動。這很可能反映了該主機上發生的活動，或與威脅行為者基礎設施產生連線並觸及該主機的網路連線。現有證據無法確定該活動的性質，但顯示該組織試圖在該機構的網絡中進行橫向移動 (TA0008)。

內部主機

ASD的ACSC調查了該機構內部網絡區段的有限數據。已知對內部組織網絡區段造成影響的惡意活動（無論是嘗試或成功）包括：攻擊者存取與VDI相關的資料、擷取內部SQL伺服器的資料 (T1505.001)，以及觀察到來自已知惡意IP地址的異常流量，通過存取閘道裝置進入網路 (TA0011)。

利用對受入侵裝置的存取權限，該組織取得了真實的使用者名稱、密碼 (T1003) 和 MFA 權杖值 (T1111)。該組織亦收集了JSON Web權杖（JWT）(T1528)，此乃用於建立虛擬桌面登入工作階段的驗證資料。攻擊者或能夠利用這些資料來

建立或劫持虛擬桌面工作階段 (T1563.002)，並以合法使用者的身分存取機構內部網絡區段 (T1078)。

攻擊者亦利用對受入侵裝置的存取權限，抓取了位於機構內部網絡的SQL伺服器資料(T1505.001)。很大機會攻擊者已取得過這些數據。

從存取閘道裝置取得的證據顯示，由已知惡意 IP 位址的網絡流量曾通過或連入該裝置。如早前所述，這顯示惡意網絡行為者已影響或利用了該裝置，並可能轉向到內部網絡。

調查時間表

下面列出調查期間所發現的關鍵活動及時間表。

時間	事件
2022年4月	已知的惡意IP位址與存取關閘主機HOST7互動。互動性質未能確定。
2022年4月	所有主機、HOST1、HOST2 和 HOST3 均受到惡意行為者的入侵，並被放置了 Web Shell。 一個日誌檔案在 HOST2 上被建立或修改。該檔案包含可能被惡意行為者擷取的憑證資料。 在HOST1和HOST3上的/etc/security/opasswd和/etc/shadow檔案遭到修改，顯示密碼曾被更改。HOST1 上的證據顯示使用者「sshuser」的密碼曾被更改。
2022年4月	HOST2 被該機構關閉。 額外的 Web Shell (T1505.003) 在 HOST1 和 HOST3 上被建立。HOST1 遭受了來自 HOST3 的 SSH 暴力破解嘗試。 一個HOST3 上的日誌檔案曾被修改。(T1070)該檔案包含憑證資料 (T1078)，很可能被惡意行為者擷取。 JWT 被擷取 (T1528) 並傳送到 HOST3 上某檔案。 HOST3 被該機構關閉。其後的所有活動均發生在 HOST1 上。
2022年4月	額外的 Web Shell在 HOST1 上被建立 (T1505.003)。JWT 被擷取並傳送到 HOST1 上某檔案。
2022年4月	額外的 Web Shell在 HOST1 上被建立 (T1505.003)，及一個已知的惡意IP位址與主機互動 (TA0011)。 一個已知的惡意IP位址與存取閘道主機HOST7互動。
2022年5月	一個已知的惡意IP位址與存取閘道主機HOST7互動(TA0011)。 在HOST1 上的日誌中顯示，一個使用者的身份驗證事件與已知的惡意 IP 位址相關聯。一個額外的 Web Shell在主機上被建立 (T1505.003)。
2022年5月	一個HOST1 上的腳本曾被攻擊者修改 (T1543)。讓腳本具備從內部 SQL 伺服器抓取資料的功能。
2022年5月	另一個HOST1上的日誌曾被修改 (T1070)。該檔案包含機構網絡的使用者名稱和密碼組合，相信是合法憑證(T1078)。
2022年5月	另一個的日誌曾被修改 (T1070)。該檔案包含從 HOST1 收集的 JWT。
2022年5月	一個額外的 Web Shell在HOST1上被建立 (T1505.003)。就在當日，該機構向 ASD 的 ACSC 通報發現一個創建日期為 2022 年 4 月的 Web Shell
2022年5月	許多腳本被創建在 HOST1 上，當中一個名為 Log4jHotPatch.jar。
2022年5月	iptables-save 指令曾被使用，在存取閘道主機新增開放兩個連接埠，分別為 9998 及 9999 (T1572)。

攻擊者的戰術和技術

以下重點介紹了調查期間辨析到的若干戰術和技術。

初始入侵

T1190 利用面向公眾的應用程式

該組織可能利用遠端存取登入及身分管理產品中的遠端程式碼執行（RCE）、權限提升及身份驗證繞過漏洞，對網絡進行初始入侵。

基於下列原因，這種初始入侵方式被認為是最有可能的：

- 伺服器當時容易受到這些 CVE的攻擊；
- 透過已知的攻擊者基礎設施，嘗試利用這些漏洞；以及
- 初次已知的內部惡意活動，發生於嘗試利用漏洞後不久。

執行

T1059.004 指令與腳本解譯器：Unix Shell

組織成功利用上述漏洞，可能在受影響的裝置上執行 Unix shell 指令。因為該裝置未有記錄相關日誌，所以無法提供攻擊者執行過的完整指令細節。

持久性

T1505.003 伺服器軟件元件：Web Shell

攻擊者在受影響裝置上部署了多個Web Shell。有可能是多個不同攻擊者部署這些Web Shell，但實際使用這些Web Shell進行活動的攻擊者數量不多。Web Shell 讓攻擊者在受入侵的裝置上任意執行指令。

權限提升

T1068 利用漏洞進行權限提升

現有證據並未能說明攻擊者取得的權限等級。然而，透過Web Shell，攻擊者很可能在受入侵裝置上的網頁伺服器取得一定等級的權限。有理由相信受入侵裝置上所存在的漏洞，使攻擊者能夠取得root權限。

存取憑證

T1056.003 輸入擷取：網頁入口擷取

受入侵裝置上的證據顯示，攻擊者已擷取數百組清楚顯示的使用者名稱及密碼，且相信是合法憑證。這些憑證很有可能是透過在真正的身份驗證過程中進行某些修改，將憑證輸出到檔案中而被擷取。

T1111 多重身份驗證攔截

攻擊者亦擷取了與合法登入相對應的 MFA 權杖值。這些資料很可能是透過在真正的身份驗證過程中進行某些修改，將資料到檔案中而被擷取。未有證據顯示儲存用於保護 MFA 權杖唯一值的「秘密伺服器」遭到入侵。

T1040 網絡監聽

有理由相信攻擊者透過擷取受入侵裝置上的 HTTP 流量來擷取 JWT。有證據顯示工具程式 tcpdump 曾在受入侵的裝置上執行，這可能是攻擊者擷取這些 JWT 的方式。

T1539 竊取 Web工作階段的Cookie

如前上所述，攻擊者擷取了 JWT，其作用類似於 Web工作階段的Cookie。攻擊者可重用這些資料以建立進一步的存取權限。

偵察

T1046 網絡服務偵察

有證據顯示網絡掃描工具 nmap曾在受入侵裝置上執行，用於掃描同一網段內的其他裝置。攻擊者很可能利用該工具以發現其他可連接的網絡服務，藉此尋找機會作橫向移動。

收集

現有證據並未能揭示攻擊者如何收集資料，或具體從受入侵裝置和其他系統中擷取了哪些資料。然而，攻擊者很有可能已有權限存取受入侵裝置上的所有檔案，包括前述的擷取憑證 (T1003)、MFA權杖值 (T1111) 及 JWT。

指揮與控制

T1071.001 應用層協定：網絡協定

攻擊者利用Web Shell以進行指揮與控制。Web shell指令將使用裝置上現有的 Web 伺服器透過 HTTPS 傳遞 (T1572)。

T1001.003 資料混淆：協定偽裝

攻擊者利用受入侵裝置作為攻擊起點，這些攻擊會與合法流量混在一起以逃避偵測。

偵測和緩解建議

ASD的ACSC強烈建議實施ASD的 八項基本控制措施 (Essential Eight) 及相關的網絡安全事件緩解策略 (Strategies to Mitgate Cyber Security Incidents)。下列是針對偵測及防止 APT40 入侵而應採取的網絡安全措施建議，接著是表 1 中總結的四個關鍵TTP的具體緩解措施。

偵測

有些被辨識的檔案是被放置在如 C:\Users\Public* 和 C:\Windows\Temp* 等位置。這些位置通常是全域可寫的，即Windows中所有註冊使用者帳戶均可存取這些目錄及其子目錄，所以非常方便寫入資料。通常，任何使用者其後都可以存取這些檔案，為橫向移動、防禦迴避、低權限執行和洩漏資料準備提供機會。

以下 Sigma 規則會偵測從可疑位置執行的動作，作為異常活動的指標。在所有情況下，均需作進一步調查以確認是否存在惡意活動及其歸因。

標題：全域可寫執行 — 臨時目錄

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

描述:偵測在 C:\Windows\Temp 的執行程序。

背景

此規則專門偵測從 C:\Windows\Temp* 目錄中執行程序Temp目錄較常被正常的應用程式所使用，作為惡意指標時，相比在 C:\Windows 中其他全域可寫子目錄的執行程序，可信度會較低。

排除由 SYSTEM 或 NETWORK SERVICE 使用者執行的應用程式，將大幅減少此規則偵測到的正常活動。

這表示此規則可能無法偵測到在較高權限層級出現的惡意執行行為，但建議搭配其他規則以判斷使用者是否嘗試將權限提升至 SYSTEM。

調查：

1. 檢查與此檔案執行直接相關的資訊，例如使用者環境、執行完整性等級、即時的後續活動，和檔案載入的圖像。
2. 調查主機上的相關進程、網絡、檔案和其他支援數據，有助判斷該活動是否惡意行為。
3. 如有需要，嘗試收集該檔案的副本進行逆向工程，以判斷其是否正當。

參考文獻：

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

作者： ASD轄下的ACSC

日期： 2024/06/19

狀態： 實驗性

標籤：

- tlp.green
- classification.au.official
- attack.execution

日誌來源：

```
category: process_creation
product: windows
```

偵測：

```
temp:
    Image|startswith:'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase:'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    User:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

```
dismhost:
    Image|endswith: 'dismhost.exe'
known_parent:
    ParentImage|endswith:
    - '\\esif_uf.exe'
    - '\\vmtoolsd.exe'
    - '\\cwainstaller.exe'
    - '\\trolleyexpress.exe'
condition: temp and not (common_temp_path or system_user or dismhost or known_parent)
```

誤報：

- 已觀察到在允許清單內的稽核應用程式會從Temp目錄執行可執行檔。
- Temp目錄內正常會包含多種安裝程式和啟動器，因此在部署此規則前，應評估該行為在受監控網絡中的普及程度（以及決定是否可將其納入在允許清單內）。

等級：低

標題：全域可寫執行 - 非-Temp 系統子目錄

ID:5b187157-e892-4fc9-84fc-aa48aff9f997

描述:偵測從 Windows 作業系統安裝目錄的子目錄中具有全域可寫子權限的位置執行程序的行為。

背景

此規則專門偵測 C:\ 以及特別是 C:\Windows* 內的全域可寫目錄，其中的執行動作，但排除 C:\Windows\Temp（因為該目錄有較多正常應用程式在使用，作為惡意指標的可信度較低）。

若檔案是以 SYSTEM 身分執行，則不應把 AppData 資料夾納入在偵測範圍內，因為許多暫存應用程式的正常執行行為均會以此方式進行。

初步完成網絡基準分析，並識別來自這些目錄的已知正常執行動作後，此規則理應鮮有觸發。

調查：

1. 檢查與該檔案執行直接相關的資訊，例如使用者環境、執行完整性等級、即時的後續活動，和檔案載入的圖像。
2. 調查主機上的相關進程、網絡、檔案和其他支援數據，有助判斷該活動是否是惡意的。
3. 如有需要，嘗試收集該檔案的副本進行逆向工程，以判斷其是否正當。

參考文獻

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

作者：ASD轄下的ACSC

日期：2024/06/19

狀態：實驗性

標籤：

- tlp.green
- classification.au.official
- attack.execution

日誌來源：

```
category: process_creation
product: windows
```

偵測：

```
writable_path:
    Image|contains:
    - ':\\$Recycle.Bin\\'
    - ':\\AMD\\Temp\\'
    - ':\\Intel\\'
    - ':\\PerfLogs\\'
    - ':\\Windows\\addins\\'
    - ':\\Windows\\appcompat\\'
    - ':\\Windows\\apppatch\\'
    - ':\\Windows\\AppReadiness\\'
    - ':\\Windows\\bcastdvr\\'
    - ':\\Windows\\Boot\\'
    - ':\\Windows\\Branding\\'
    - ':\\Windows\\CbsTemp\\'
    - ':\\Windows\\Containers\\'
    - ':\\Windows\\csc\\'
    - ':\\Windows\\Cursors\\'
    - ':\\Windows\\debug\\'
    - ':\\Windows\\diagnostics\\'
    - ':\\Windows\\DigitalLocker\\'
    - ':\\Windows\\dot3svc\\'
    - ':\\Windows\\en-US\\'
    - ':\\Windows\\Fonts\\'
    - ':\\Windows\\Globalization\\'
    - ':\\Windows\\Help\\'
    - ':\\Windows\\IdentityCRL\\'
    - ':\\Windows\\IME\\'
    - ':\\Windows\\ImmersiveControlPanel\\'
```

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
User:'SYSTEM'

condition: writable_path and not appdata

誤報

已觀察到在允許清單內的稽核應用程式會從這些目錄執行可執行檔。

在這些目錄中，有可能存有用於受監控環境下的腳本和管理工具，故此應按個別情況處理。

等級：高

標題：全域可寫入的執行活動 – Users

ID:6dda3843-182a-4214-9263-925a80b4c634

描述:偵測執行的程序：從 C:\Users\Public* 以及Users目錄下其他全域可寫入的資料夾

背景

若檔案是以 SYSTEM 身分執行，則AppData 資料夾會被排除在外，這是一種許多暫存應用程式檔案被執行的正常方式。

調查：

1. 檢查與該檔案執行直接相關的資訊，例如使用者環境、執行完整性等級、即時的後續活動，和檔案載入的圖像。
2. 調查主機上的相關進程、網絡、檔案和其他支援數據，有助判斷該活動是否是惡意的。
3. 如有需要，嘗試收集該檔案的副本進行逆向工程，以判斷其是否正當。

參考文獻

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

作者： ASD轄下的ACSC

日期： 2024/06/19

狀態： 實驗性

標籤：

- tlp.green
- classification.au.official
- attack.execution

日誌來源：

category: process_creation
product: windows

偵測：

```
users:
    Image|contains:
    - ':\\Users\\All Users\\'
    - ':\\Users\\Contacts\\'
    - ':\\Users\\Default\\'
    - ':\\Users\\Public\\'
    - ':\\Users\\Searches\\'
appdata:
    Image|contains: '\\AppData\\'
    User:'SYSTEM'
condition: users and not appdata
```

誤報

- 在Public目錄或其子目錄中，有可能存有用於受監控環境下的腳本和管理工具，故此應按個別情況處理。

等級：中

緩解措施

日誌記錄

在ASD的ACSC調查期間，一個常見的問題是缺乏涵蓋多個範疇的全面及具歷史紀錄的日誌，包括 Web伺服器請求日誌、Windows事件日誌及互聯網代理伺服器日誌，從而削弱了調查工作的效率與成效。

ASD的ACSC建議審視和實施其有關 Windows 事件日誌記錄和轉送 (Windows Event Logging and Forwarding) 的指引，包括 Windows 事件日誌記錄儲存庫 (Windows Event Logging Repository) 中的設定檔和腳本，以及《資訊安全手冊》的 系統監控指引 (guidelines for System Monitoring)，內容涵蓋將日誌集中管理及保留日誌至適當期限。

修補更新管理

應迅速更新所有暴露於互聯網的裝置與服務，包括Web伺服器、Web應用程式及遠端存取閘道等。建議考慮實施一個中央的程式更新管理系統，令過程更自動化和迅速。ASD的ACSC建議實施《資訊安全手冊》中關於 系統管理指引 (Guidelines for System Management)，特別是當中適用於系統修補的控制措施。

攻擊者所利用的大部分都是公開已知的漏洞，並已有相應修補更新或緩解措施可用。機構應確保針對暴露於互聯網上的基礎設施，能在 48 小時內套用安全修補更新或緩解措施，並在可行情況下，採用最新版本的軟件與作業系統。

網絡分段

網絡分段可大幅提高攻擊者找到和存取機構敏感資料的難度。透過拒絕電腦之間的通訊（如非必要）來把網絡分段，以限制或阻止橫向移動。重要的伺服器，例如Active Directory及其他身份驗證伺服器，應只可經由少數的中介伺服器（即「跳板伺服器」）進行管理。上述伺服器應實施嚴格監控、確保安全，並對可連接的使用者和裝置有所限制。

縱使在部份情況下未能得知有否成功阻止橫向移動，額外的網絡分段都可能進一步限制攻擊者能存取和擷取的資料量。

其他緩解措施

撰寫機構也建議採取下列緩解措施，以打擊 APT40 和其他攻擊者使用的 TTP。

- 停用未使用或不必要的網絡服務、連接埠和協定。
- 使用經妥善調校的Web應用程式防火牆（WAF）來保護Web伺服器及應用程式。
- 強制實行最小權限原則，限制對伺服器、檔案分享及其他資源的存取。
- 使用多重身份驗證 (MFA) 和管理服務帳戶，令憑證更難被破解和重複使用。MFA 應套用至所有可透過網際網絡存取的遠端服務，包括：
  - Web 及雲端電郵服務
  - 協作平台
  - 虛擬私人網絡（VPN）連線
  - 遠端桌面服務
- 更換所有已達支援終止的裝置。

圖表 1：緩解策略／技術

TTP	Essential Eight Mitigation Strategies (八大核心緩解措施)	資訊安全手冊 (ISM) 控制措施
初始入侵 T1509 入侵面向公眾的應用程式	更新修補應用程式 更新修補作業系統 多重身份驗證 應用程式控制	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
執行 T1059 指令及腳本解譯器	應用程式控制 限制 Microsoft Office 巨集功能 限制管理權限	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
持久性 T1505.003 伺服器軟件元件Web Shell	應用程式控制 限制管理權限	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
初始入侵 / 權限提升 / 持久性 T1078 有效帳戶	更新修補作業系統 多重身份驗證 限制管理權限 應用程式控制 使用者應用程式的強化	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

如需更多一般檢測和緩解建議，請參閱 MITRE ATT&CK 技術網頁上的緩解和檢測 (Mitigations and Detection) 部分，以了解本公告末尾 MITRE ATT&CK 摘要中提及的各種技術。

免責聲明

本報告中的資訊按「原樣」提供，僅供參考。撰寫機構並非支持任何商業實體、產品、公司或服務，包括文件中提及的任何實體、產品或服務。任何被提及的商業實體、產品、流程或服務，或其服務標記、商標、製造商或其他方式，並不構成或暗示撰寫機構對其的認可、推薦或偏好。

本文件標註為 TLP:CLEAR (透明級別) 披露不受限制當資訊被濫用的風險極小或沒有可預見的風險時，消息來源可以被標示作 TLP:CLEAR 級別，並根據適用的規則和程序進行公開發布。根據標準版權規定，TLP：CLEAR 資訊的分發並不受限制。有關TLP (交通燈協定) 的更多資料，請前往 cisa.gov/tlp

MITRE ATT&CK – APT40 曾使用且值得關注的攻擊技術

偵察 (TA0043)	
搜尋受害者擁有的網站 (T1594)	收集受害者的身份資訊：憑證資料 (T1589.001)
主動掃描：漏洞掃描 (T1595.002)	收集受害者的主機資訊 (T1592)
搜尋公開的網站/網域：搜尋引擎 (T1593.002)	收集受害者網絡資訊：網域屬性 (T1590.001)
收集受害者網絡資訊：電郵地址 (T1589.002)	

資源開發 (TA0042)	
取得基礎設施網域 (T1583.001)	取得基礎設施 (T1583)
取得基礎設施DNS 伺服器 (T1583.002)	入侵帳戶 (T1586)
發展能力：程式碼簽章憑證 (T1587.002)	入侵基礎設施 (T1584)
發展能力：數碼憑證 (T1587.003)	發展能力：惡意軟件 (T1587.001)
取得能力：程式碼簽章憑證 (T1588.003)	建立帳戶：雲端帳戶 (T1585.003)
入侵基礎設施：網絡裝置 (T1584.008)	取得能力：數碼憑證 (T1588.004)

初始入侵 (TA0001)	
有效帳戶 (T1078)	網絡釣魚 (T1566)
有效帳戶：預設帳戶 (T1078.001)	網絡釣魚：定向釣魚郵件附件 (T1566.001)
有效帳戶：網域帳戶 (T1078.002)	網絡釣魚：定向釣魚郵件連結 (T1566.002)
外部遠端服務 (T1133)	利用面向公眾的應用程式漏洞 (T1190)
順路入侵 (T1189)	

執行階段 (TA0002)	
Windows 管理工具 (T1047)	指令及腳本解譯器：Python (T1059.006)
排程任務/作業：At 指令排程 (T1053.002)	指令及腳本解譯器：JavaScript (T1059.007)
排程任務/作業：排程任務 (T1053.005)	本地API (T1106)
指令及腳本解譯器 (T1059)	進程間通訊 (T1559)
指令及腳本解譯器：Windows命令提示字元 (T1059.003)	系統服務：服務執行 (T1569.002)
指令及腳本解譯器：PowerShell (T1059.001)	利用用戶端執行漏洞 (T1203)
指令及腳本解譯器：Visual Basic (T1059.005)	使用者執行：惡意檔案執行 (T1204.002)
指令及腳本解譯器：Unix Shell (T1059.004)	指令及腳本解譯器：Apple Script (T1059.002)
排程任務/作業：Cron排程 (T1053.003)	軟件部署工具 (T1072)

持久性 (TA0003)	
有效帳戶 (T1078)	伺服器軟件組件Web Shell (T1505.003)
Office 應用程式啟動：Office 模板巨集 (T1137.001)	建立或修改系統程序Windows 服務 (T1543.003)
排程任務/作業：At 指令排程 (T1053.002)	開機或登入自動啟動執行登錄檔啟動鍵 / 啟動資料夾 (T1547.001)
排程任務/作業：排程任務 (T1053.005)	開機或登入自動啟動執行捷徑修改 (T1547.009)
外部遠端服務 (T1133)	劫持執行流程：DLL 搜尋順序劫持 (T1574.001)
排程任務/作業：Cron排程 (T1053.003)	劫持執行流程：DLL 側載 (T1574.002)
帳戶操控 (T1098)	有效帳戶：雲端帳戶 (T1078.004)
有效帳戶：網域帳戶 (T1078.002)	

權限提升 (TA0004)	
排程任務/作業：At 指令排程 (T1053.002)	建立或修改系統程序Windows 服務 (T1543.003)
排程任務/作業：排程任務 (T1053.005)	開機或登入自動啟動執行登錄檔啟動鍵 / 啟動資料夾 (T1547.001)
程序注入執行線程劫持 (T1055.003)	開機或登入自動啟動執行捷徑修改 (T1547.009)
程序注入程序空洞化 (T1055.012)	劫持執行流程：DLL 搜尋順序劫持 (T1574.001)

權限提升 (TA0004)	
有效帳戶：網域帳戶 (T1078.002)	利用漏洞進行權限提升 (T1068)
存取權杖操控：權杖冒充／竊取 (T1134.001)	事件觸發執行：Unix Shell 設定修改 (T1546.004)
程序注入動態連結程式庫注入 (T1055.001)	有效帳戶：網域帳戶 (T1078.002)
有效帳戶：本機帳戶 (T1078.003)	

迴避防禦 (TA0005)	
Rootkit (T1014)	間接指令執行 (T1202)
混淆的檔案或資訊 (T1027)	系統二進位代理執行：Mshta (T1218.005)
混淆的檔案或資訊：軟件封裝 (T1027.002)	系統二進位代理執行：Regsvr32 (T1218.010)
混淆的檔案或資訊：隱寫術 (T1027.003)	攪亂信任控制：簽署程式碼 (T1553.002)
混淆的檔案或資訊：傳送後編譯 (T1027.004)	檔案及目錄權限修改：Linux 及 Mac 檔案與目錄權限修改 (T1222.002)
偽裝：偽裝合法名稱或位置 (T1036.005)	虛擬化／沙盒迴避：系統檢查 (T1497.001)
程序注入執行線程劫持 (T1055.003)	偽裝 (T1036)
反射式代碼加載 (T1620)	弱化防禦：停用或修改系統防火牆 (T1562.004)
程序注入：程序空洞化 (T1055.012)	隱藏痕跡：隱藏檔案及目錄 (T1564.001)
指標清除：檔案刪除 (T1070.004)	隱藏痕跡：隱藏視窗 (T1564.003)
指標清除：時間戳竄改 (T1070.006)	劫持執行流程：DLL 搜尋順序劫持 (T1574.001)
指標清除：清除 Windows 事件日誌 (T1070.001)	劫持執行流程：DLL 側載 (T1574.002)
修改登錄檔 (T1112)	網絡服務 (T1102)
解混淆／解碼檔案或資訊 (T1140)	偽裝：偽裝任務或服務 (T1036.004)
弱化防禦 (T1562)	

憑證存取 (TA0006)	
作業系統憑證擷取：LSASS 記憶體 (T1003.001)	不安全憑證：檔案中的憑證 (T1552.001)
作業系統憑證擷取：NTDS (T1003.003)	暴力破解：密碼猜測 (T1110.001)
網絡封包攔截 (T1040)	強制驗證 (T1187)

憑證存取 (TA0006)	
從密碼存儲中取得憑證：鑰匙串 (T1555.001)	竊取或偽造 Kerberos 票據：Kerberoasting (T1558.003)
輸入捕獲：鍵盤記錄 (T1056.001)	多重身份驗證攔截 (T1111)
竊取網頁工具階段 Cookie (T1539)	竊取應用程式存取權杖 (T1528)
利用漏洞進行憑證存取 (T1212)	暴力破解：密碼破解 (T1110.002)
輸入捕獲：網頁入口捕獲 (T1056.003)	作業系統憑證擷取：DCSync (T1003.006)
從密碼存儲中取得憑證 (T1555)	從密碼存儲中取得憑證：瀏覽器憑證 (T1555.003)

偵察 (TA0007)	
系統服務偵察 (T1007)	系統資訊偵察 (T1082)
應用視窗偵察 (T1010)	帳戶偵察：本機帳戶 (T1087.001)
查詢登錄檔 (T1012)	系統資訊偵察，技術 T1082 – 企業 | MITRE ATT&CK®
檔案及目錄偵察 (T1083)	系統時間偵察 (T1124)
網絡服務偵察 (T1046)	系統擁有者／使用者偵察 (T1033)
遠端系統偵察 (T1018)	網域信任偵察 (T1482)
帳戶偵察：電郵帳戶 (T1087.003)	帳戶偵察：網域帳戶 (T1087.002)
系統網絡連線偵察 (T1049)	虛擬化／沙盒迴避：系統檢查 (T1497.001)
程序偵察 (T1057)	軟件偵察 (T1518)
權限群組偵察：網域群組 (T1069.002)	網絡共享偵察，技術 T1135 – 企業 | MITRE ATT&CK®
系統網絡配置偵察：網際網絡連線偵察 (T1016.001)	

橫向移動 (TA0008)	
遠端服務：遠端桌面協定 (T1021.001)	遠端服務 (T1021)
遠端服務：SMB／Windows 管理共享 (T1021.002)	使用替代的驗證資料：傳遞票證 (T1550.003)
遠端服務：Windows 遠端管理 (T1021.006)	橫向工具傳輸 (T1570)

收集 (TA0009)	
本機系統資料 (T1005)	封存收集所得的資料：透過程式庫封存 (T1560.002)
來自網絡共享磁碟的資料 (T1039)	電郵收集：遠端電郵收集 (T1114.002)

收集 (TA0009)	
輸入捕獲：鍵盤記錄 (T1056.001)	剪貼簿資料 (T1115)
自動化收集 (T1119)	來自資訊儲存庫的資料 (T1213)
輸入捕獲：網頁入口捕獲 (T1056.003)	預存資料：遠端資料預存 (T1074.002)
預存資料：本機資料預存 (T1074.002)	封存收集所得的資料 (T1560)
電郵收集 (T1114)	

資料外傳 (TA0010)	
透過指揮及控制頻道外傳 (T1041)	透過替代協定外傳：透過非對稱加密的非指揮及控制協定外傳 (T1048.002)
透過替代協定外傳 (T1048)	透過網絡服務外傳：外傳至雲端儲存

指揮與控制 (TA0011)	
資料混淆：協定冒充 (T1001.003)	網絡服務：死信解析器 (T1102.001)
常用通訊埠 (T1043)	網絡服務：單向通訊 (T1102.003)
應用層協定：網頁協定 (T1071.001)	工具傳輸入口 (T1105)
應用層協定：檔案傳輸協定 (T1071.002)	代理：內部代理 (T1090.001)
代理：外部代理 (T1090.002)	非標準通訊埠 (T1571)
代理：多跳代理 (T1090.003)	協定隧道 (T1572)
網絡服務：雙向通訊 (T1102.002)	加密通道 (T1573)
加密通道：非對稱加密 (T1573.002)	工具傳輸入口 (T1105)
代理，技術 T1090 – 企業 | MITRE ATT&CK®	

影響 (TA0040)	
服務停止 (T1489)	磁碟清除 (T1561)
系統關機／重開 (T1529)	資源劫持 (T1496)

筆記

免責聲明

本指南的內容只屬一般性資料，不應被視為法律建議，或是在任何特定或緊急情況下依賴作為幫助。在任何重要事項上，您都應該根據個人情況，尋求適當的獨立專業建議。

若因依賴本指南的資訊而引致任何損害、損失或費用，聯邦政府是不會承擔任何責任或義務的。

國徽的使用

總理和內閣部網站的 聯邦國徽資訊和指南 | pmc.gov.au 詳細說明了國徽使用的條款。

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