# 109年第3季資通安全技術報告

Quarterly Technical Report

# 目　次

# 圖 目 次

# 摘要

「第 3 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關最新資安風險之關注重點。

「第 3 季資通安全技術報告」分為以下 4 個章節。

●1.資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為加拿大政府網站遭駭客攻擊；另一起案例為駭客挾持 Tor 流量，以竊取比特幣。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 52.39%) 類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」 (占 10.2%)與「設備問題」(占 3.06 %)為主要通報類型。

●2.資安專題分享

資安專題分享主題為 DLL Side Loading 攻擊手法簡介，資安廠商 Cymulate 發現可利用微軟遠端桌面應用程式之 DLL Side Loading 漏洞，讓駭客執行遠端程式碼。藉由此攻擊手法驗證實作與運用，呼籲管理者應針對應用程式安裝目錄或免安裝程式目錄，檢視應用程式所呼叫使用之 DLL 是否有合法簽章與檔案目錄是否存有與系統目錄中相同名稱之 DLL 檔案。

●3.資安技術研析

資安技術研析主題為 Mustang Panda 族群追蹤與樣態分析，彙整相關案件攻擊手法，發現 Mustang Panda 族群發送以 COVID-19 為主題之社交工程郵件，藉由附件之惡意程式，入侵且操控受害電腦。案例分析發現該族群是以對外服務網站做為攻擊目標植入網頁後門，利用離地攻擊(Living

off the Land, LotL)手法於內部擴散，植入 Cobalt Strike 類型後門，以 HTTP/DNS 兩種管道控制受害主機。

●4.結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享 DLL Side Loading 攻擊手法，提醒系統管理者應有之防範作為，並應隨時注意系統更新訊息。此外，資安技術研析主題為分析 Mustang Panda 族群追蹤與樣態，整理相關攻擊手法，提醒機關及早準備因應策略與行動方案。

# 1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因與可能之衝擊與影響。109 年第 3 季(以下簡稱本季)探討憑證填充攻擊(Credential Stuffing)，該攻擊是以自動化方式運用不當獲得之帳密嘗試登入網路服務之攻擊技巧。駭客憑藉使用者外洩之個人資料，持續試圖登入不同網路服務。另外，面對網路提供各式各樣之服務，在連線前之資通安全意識，除不使用相同之帳號密碼外，亦應先行檢視網路服務提供者是否使用強制安全傳輸技術機制，以確保連線資料傳輸之安全。

本章節之事件與議題皆配合整理相關之資安防護重點，提供組織就相關資安風險或議題進行評估，並依循資安防護重點進行強化。

## 1.1 全球資安威脅現況

帳號密碼可以說是資通安全第一道防線，而現今駭客利用憑證填充攻擊，利用網路世界大量外流之個人資料、電子郵件或帳號密碼，試圖利用免費或購買之憑證，入侵相關網路或應用服務。再加上使用者習慣使用相同之帳號密碼組合於不同存取服務上，也大大提升駭客攻擊成功之機率。

另外，持續宣導服務網站提供加密之安全傳輸機制，亦是刻不容緩。未加密之網路連線，可能面臨中間人攻擊。若遭遇相關攻擊，則駭客不僅能從未加密通訊中成功截取或接收資料，甚或可能竄改資料，造成更大損失。

本季具指標性案例為加拿大政府網站遭駭客攻擊，竊取上萬用戶憑證；另一起案例為駭客挾持 Tor 流量，以竊取比特幣。

首先，探討案例為加拿大政府網站遭駭客竊取上萬用戶憑證。駭客鎖定該國政府所提供之身分驗證服務 GCKey 憑證與國稅局(Canada Revenue Agency, CRA)帳戶發動網路攻擊，估計約有 9 千多筆 GCKey 憑證與 5 千多筆 CRA 帳號遭破解，當局已緊急關閉受駭帳號，並要求用戶重新更換

密碼。

加拿大政府表示，駭客透過憑證填充攻擊竊取 GCKey 憑證與 CRA 帳戶，該攻擊係利用殭屍網路(botnet)，以自動化方式，使用先前已外洩之登入帳號與密碼試圖登入網路服務，加上使用者習慣為求便利，在不同服務上使用相同密碼之特性，遭駭客利用成功竊取 9,041 筆 GCKey 憑證與 5,500 筆 CRA 帳戶，且駭客企圖利用受駭憑證存取相關服務。

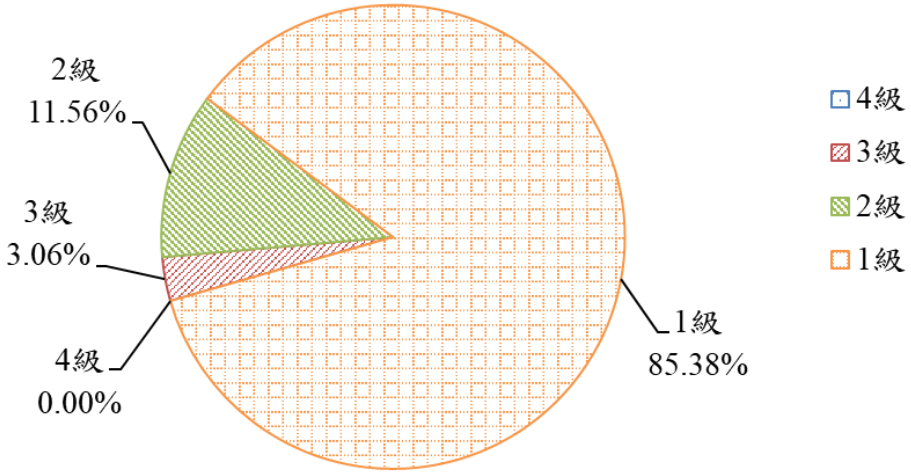
第 2 起案例為駭客挾持 Tor 流量以竊取比特幣，資安研究人員指出，洋蔥路由(The Onion Router, Tor)網路存在大量惡意出口節點，駭客可藉由 SSL Strip 手法，進行中間人攻擊取得網路傳輸資訊，當發現造訪目標為 Bitcoin Mixer 服務時，即發動攻擊並透過置換使用者所輸入之錢包位址，竊取比特幣。

Tor 網路為開源之匿名傳輸網路架構，透過散布在全球逾 7,000 個志願節點傳遞流量，藉此躲避追蹤與流量分析。由於 Tor 網路並未嚴格審核該網路上之節點，使駭客得以部署惡意出口節點，進而挾持使用者連線至特定網站之流量。截至本年 8 月，仍有超過 10%之出口節點被駭客操縱。駭客透過 SSL Strip 手法，攻擊連線至 Bitcoin Mixer 服務之流量，Bitcoin Mixer 服務可協助使用者將比特幣於不同錢包中進行轉移；而 SSL Strip 攻擊為駭客介入 HTTPS 流量，並將其變更為 HTTP 流量之過程，讓駭客得以存取未加密之網頁流量，透過置換 Tor 網路使用者所輸入之目標錢包位址，藉此盜走比特幣。

綜覽本季重大資安事件，面對憑證填充攻擊除應持續加強宣導，使用者避免在不同網站上使用相同之帳號密碼組合，就服務提供者亦應加強身分認證之管理，如採用雙因子認證機制提高身分鑑別之準確度。

## 1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成之衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 85.38%為大宗，2 級事件占 11.56%次之，3 級事件僅占 3.06%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。



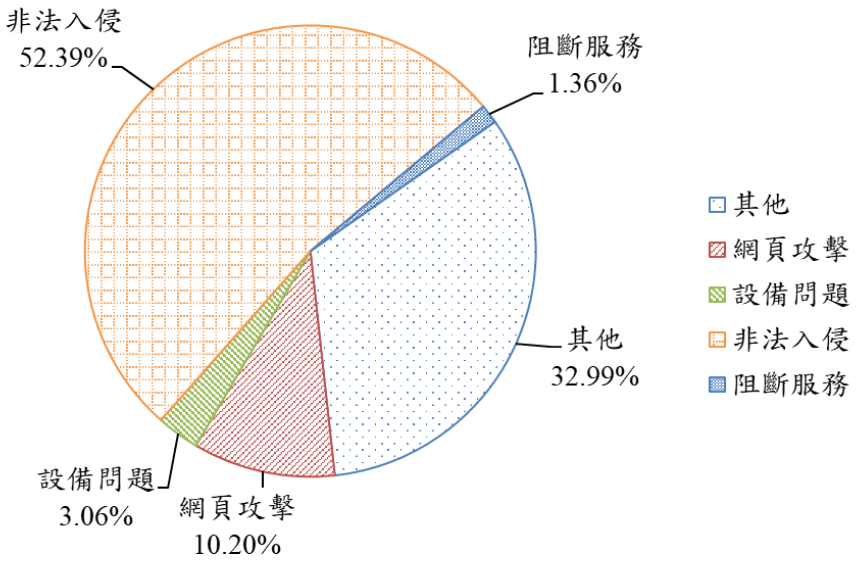

資料來源：本報告整理

圖1　109 年第 3 季通報事件影響等級比率圖

本季接獲之 3 級重要通報事件，發現部分機關網站提供民眾上傳檔案功能，因未限制檔案類型，進而遭駭客利用上傳惡意程式。另一起事件為機關利用 Google 表單提供民眾登記，惟 Google 表單權限設定錯誤，導致可檢索其他登記民眾資料，如電子信箱、姓名及身分證字號等個人資料。這些案例顯示，隨著 e 化服務系統普及，越來越多便民服務，亦象徵著在設定組態上安全規劃應有更嚴謹之管理程序。

除上述資安事件外，本季通報案件發現駭客利用開發或維護商做為攻擊機

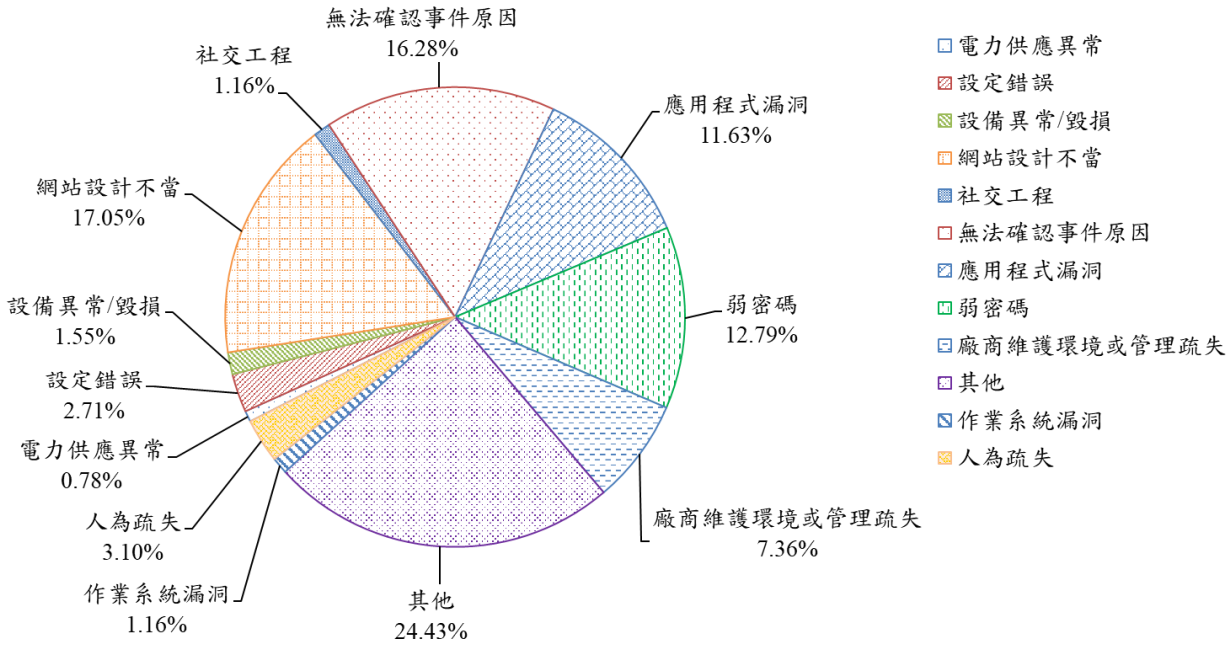
關跳板，駭客先行入侵開發或維護商成功竊取其遠端登入之系統帳號密碼，再透過其網路環境遠端存取機關資訊設備，進而植入惡意程式，藉由這些入侵途徑，也突顯非法入侵在事件比率上一直居高不下。整體事件比率，以「非法入侵」(占 52.39%)類型為主，排除綜合類型「其他」外，「網頁攻擊」與「設備問題」類型次之，詳見圖 2。




資料來源：本報告整理

圖2　109 年第 3 季通報類型比率圖

最後，分析通報事件發生原因，以其他(24.43%)、無法確認事件原因(16.28%)及網站設計不當(17.05%)位居前三名，其次分別為弱密碼(12.79%)、應用程式漏洞(11.63%)、廠商維護環境或管理疏失(7.36%)、人為疏失(3.1%)、設定錯誤(2.71%)、作業系統漏洞(1.16%)、設備異常/毀損(1.55%)、社交工程(1.16%)及電力供應異常(0.78%)，詳見圖 3。本季一般事件發生原因以其他與無法確認事件原因為主，通常是因為部分通報事件發生後，因時間因素而無法判斷初始肇因，另外，本季依然觀測到有因監視器設備受害狀況，再加上設備受限無法存放日誌紀錄，故以「無法確認事件原因-無相關紀錄可供檢視」進行結案，相比上季事件統計已明顯下降。




資料來源：本報告整理

圖3　109 年第 3 季通報事件發生原因比率圖

分析第 3 季通報事件發生原因，發現除因系統日誌無法保留較長時間，致無法追溯事件發生原因。同時，亦有資安事件是因存放在記憶體中之暫存檔累積過多，致未有足夠記憶體可執行相關程式，導致系統異常，甚至連線中斷事件發生。

## 1.3 資安防護重點

分析本季全球資安威脅現況，發現一旦個人資料外洩，特別是帳號與密碼，隨著網路免費分享或有利可圖等動機下，造成之影響與衝擊逐漸擴大。以加拿大政府網站遭駭客竊取上萬用戶憑證為例，駭客獲得相關個人憑證後，又利用使用者慣用之帳號與密碼組合，進而存取其他相關服務。

另一個值得注意之資通安全議題為網路通訊安全，組織在使用開源傳輸網路時應先審慎評估，應先就傳輸資料機敏程度進行評估，是否適合在開源網路架構上傳輸，以及應用時是否有配套之傳輸與資料加密機制。

分析政府機關通報事件發現，3級資安事件仍以個人資料外洩為大宗。而外洩原因，人為疏失是近來討論議題之一。任何資安防護措施，在百密一疏情況下，就有可能造成資安破口，因此不論是委外廠商或內部人員錯誤設定，其實皆需要系統管理者或使用者有足夠之資通安全素養，方能提升整體之資安防禦。

綜整以上資安威脅現況，提供資安防護建議如下：

●憑證填充攻擊資安管理

– 監測網路流量與系統登入狀況，依資源考量搭配建置異常行為分析系統。

– 資通系統建置雙重認證之資安機制，提升身分識別與鑑別完備度。

– 資通系統強制定期變更密碼，教育使用者在不同網路服務或資通系統登入時，應使用不同帳號與密碼組合。

●開源網路或軟體資安管理

– 公告開源網路或軟體使用之政策與執行程序等資通安全管理規範。

– 核定內部可使用之開源網路、軟體，定期檢視相關更新。

– 定期進行弱點掃描與漏洞修補作業，必要時執行風險評估以檢視風險回應作業。

●系統日誌資安管理

– 依資通系統分級，訂定日誌時間週期、紀錄留存及暫存檔清理程序。

– 訂定日誌或暫存檔之管理規範，包含儲存容量、存取規則及清理原則等。

– 強化資通系統容量與使用狀況之監控作業，持續優化管理作業。

# 2. 資安專題分享_ DLL Side Loading 攻擊手法簡介

動態連結函式庫(Dynamic-link library, DLL)是微軟在 Windows 作業系統中實現共享函式庫之方式，近期以色列資安廠商 Cymulate 發現利用微軟遠端桌面應用程式之 DLL Side Loading 漏洞，可讓駭客執行遠端程式碼。根據微軟表示「應用程序目錄 DLL 植入，被視為是深度防禦問題，僅在以後的版本中才會考慮進行更新」，因此現階段仍存在可利用 DLL Side Loading 攻擊手法。

以下將說明 Windows 桌面應用程式載入 DLL 時之搜尋順序，並藉由實作驗證利用此搜尋順序，進行 DLLSideLoading 攻擊手法。

## 2.1 DLL Side Loading 攻擊

執行 Windows 桌面應用程式時，會依下列順序搜尋所需要之 DLL 檔，當在某個位置順利找到需載入之 DLL 檔便結束搜尋，或所有位置都搜尋過仍無該 DLL 檔，亦會結束搜尋，詳見圖 4。

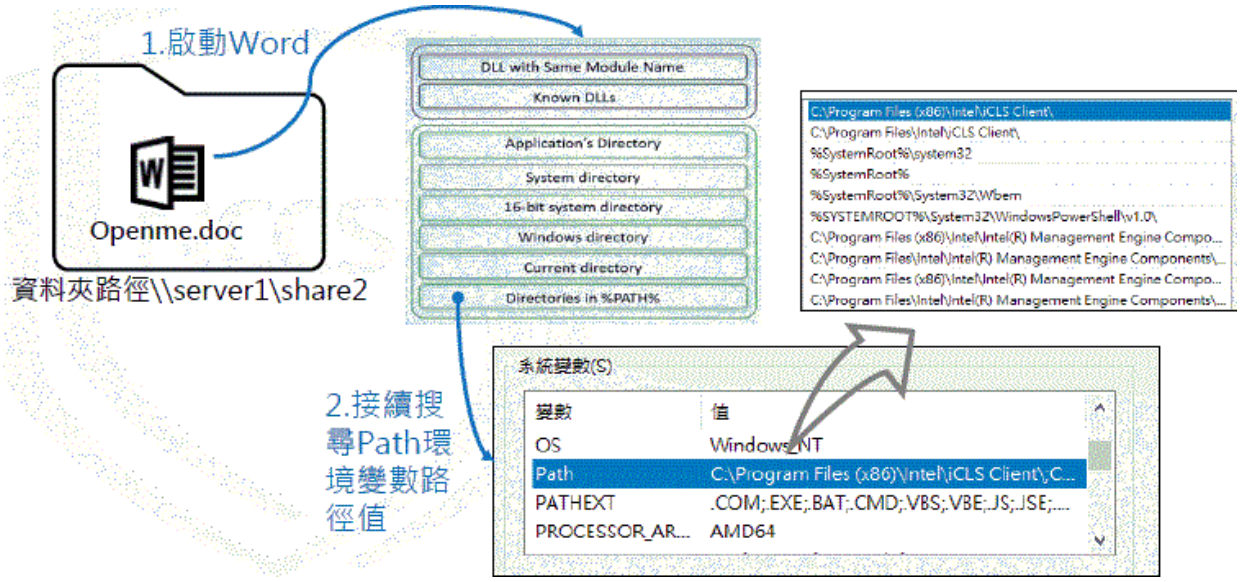
| 搜尋順序 | 搜尋位置 |
|---|---|
| 1 | 已載入記憶體之同模組名之DLL |
| 2 | Windows Known DLLs列表 |
| 3 | 應用程式所在目錄 |
| 4 | 系統目錄 |
| 5 | 16位元系統目錄 |
| 6 | Windows目錄 |
| 7 | 當下目錄 |
| 8 | 環境變數PATH中列出的目錄 |

資料來源：本報告整理

圖4　DLL 搜尋順序

如果記憶體中已有相同名稱之 DLL 檔，則直接使用記憶體中之 DLL，則

不再搜尋。如果 DLL 名稱列於 Known DLLs 列表中，則必須使用此列表中之 DLL。列表存放路徑為 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs，須具備 System 權限方可修改此列表。可依搜尋順序 3「應用程式所在目錄」權限管理情形，區分被利用執行攻擊時是否需要提權，若為安裝路徑受權限控管，則存取需提權。另一種狀況為安裝路徑未受權限控管，則不需提權。舉例來說，當使用者從\\server1\share2\路徑打開一個.doc 文件將啟動 Microsoft Word，如果 Microsoft Word 在受信任位置找不到其依賴之 DLL「OART.dll」，將嘗試從當下目錄載入。當前 7 個位置仍未找到欲載入之 DLL 時，最後將依 Path 環境變數路徑值進行 DLL 搜尋。詳見圖 5。



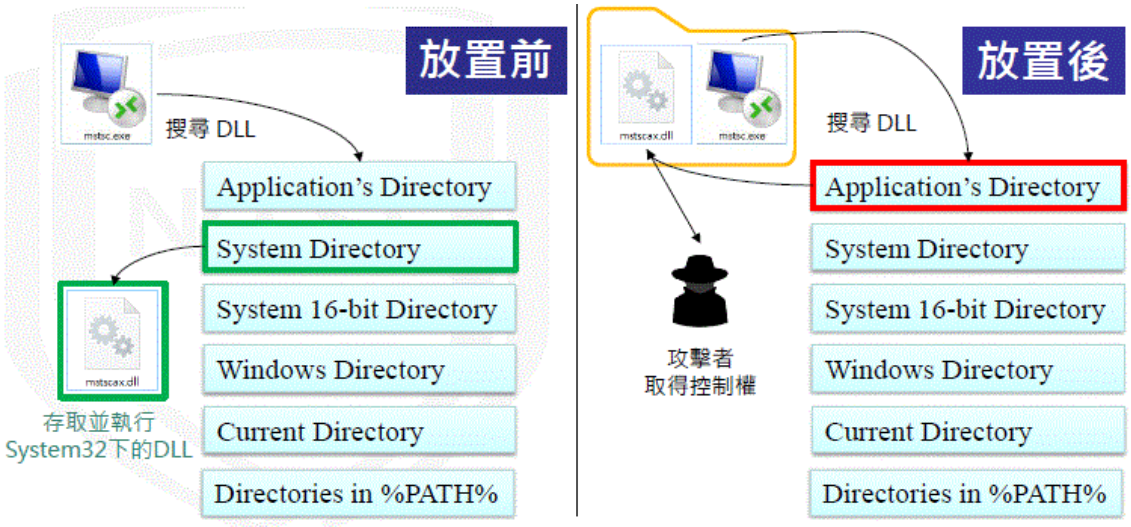

資料來源：本報告整理

圖5　依 Path 環境變數路徑值進行 DLL 搜尋

DLL Side Loading 攻擊能成功最主要之因素，攻擊者若能將相同名稱之惡意 DLL 放置於搜尋順序較正常 DLL 前之位置，讓應用程式優先載入，即有攻擊成功機會。

## 2.2 攻擊手法驗證實作與運用

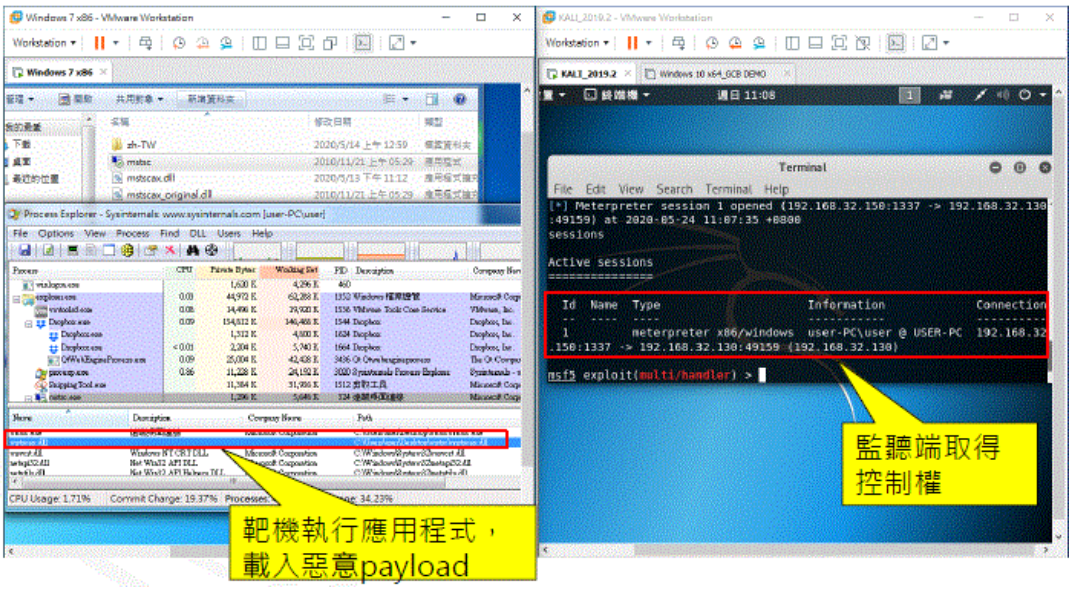
實作情境一開始會先建立一個含有遠端桌面執行程式之獨立資料夾，並於該路徑下放置「mstascx.dll」payload，驗證執行遠端桌面程式後，攻擊者可取得控制權，詳見圖 6。




資料來源：本報告整理

圖6　放置「mstascx.dll」payload

第一步驟製作 DLL 格式之惡意 payload，接續將惡意 DLL 放置於執行檔路徑，更改 DLL 檔案名稱為 mstscax.dll，並與遠端桌面應用程式放置於相同資料夾。下一步驟，則設定 metasploit 監聽端。最後執行應用程式，攻擊者取得控制權，詳見圖 7。




資料來源：本報告整理

圖7　成功取得控制權

經研析，並非只有遠端桌面應用程式可進行 DLL Side Loading 攻擊，亦可透過 TeamViewer 等免安裝工具。攻擊者將含有惡意 payload 之 TeamViewer 免安裝工具，放置於 Internet 供一般使用者下載，使用者執行含有惡意 payload 之 TeamViewer 後，攻擊者則可取得控制權限。另一種攻擊範例為搭配 WinRAR 之 CVE-2018-20250 漏洞，將 Zoom 更新說明文件與檔名為「cryptbase.dll」之惡意 payload 封裝成一個壓縮檔。使用者收到壓縮檔後，使用 WinRAR 進行解壓縮時，將植入「cryptbase.dll」至 Zoom 安裝路徑。日後每當執行 Zoom 應用程式時，將優先載入該 DLL，攻擊者則順利取得控制權。

針對此攻擊手法，應針對應用程式安裝目錄或免安裝程式目錄，特別檢視應用程式所呼叫使用之 DLL 是否有合法簽章，以及檔案目錄是否存有與系統目錄中相同名稱之 DLL 檔案。同時，持續關注應用程式開發廠商進度，如有釋出更新程式，則應儘速安裝。

# 3.資安技術研析_ Mustang Panda 族群追蹤與樣態分析

本季所探討之資安技術研析為 Mustang Panda 族群追蹤與樣態分析，技服中心於外部情資發現以利用武漢肺炎為題，企圖攻擊台灣之惡意程式樣本，分析其背後發動組織為 Mustang Panda。

Mustang Panda 攻擊活動最早被揭露是在 107 年 6 月由網路安全服務公司 CrowdStrike 公開情資分享，該族群攻擊目標包含緬甸、越南、巴基斯坦、蒙古非政府組織、美國智庫單位等。

## 3.1 攻擊案例與惡意程式樣態分析

Mustang Panda 慣用手法為善於利用 windows 捷徑檔(.lnk)執行特定腳本，啟動包含 PlugX、Cobalt Strike 等共用形態之後門程式對外通聯。關聯分析該族群近期活動，於本年 2 月至 4 月期間發動兩波與台灣相關攻擊，第一階段推測以寄送 COVID-19 為題之社交工程郵件為主，以離地攻擊(LotL)多層次封裝方式，最終將後門以無檔案方式(fileless)啟動，第二階段則以網站攻擊為主要目標，無特殊封裝，後門落地。

彙整相關案件攻擊手法，均是以對外服務網站做為攻擊目標，植入網頁後門，利用離地攻擊手法於內部擴散，植入 Cobalt Strike 類型後門，以 HTTP/DNS 兩種管道控制受害主機，案例攻擊手法，詳見圖 8。


資料來源：本報告整理

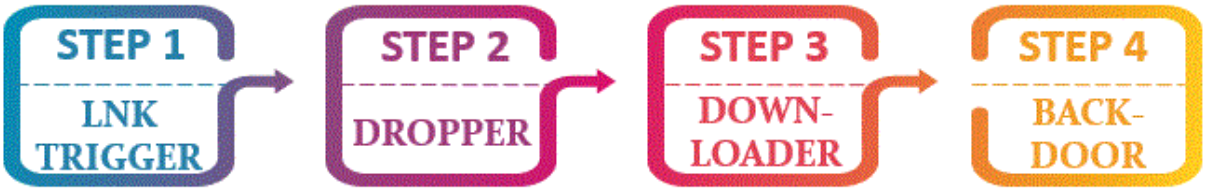
圖8　Mustang Panda 案例攻擊手法

## 3.2 惡意程式樣態分析

以下透過兩種相關關聯分析，說明 Mustang Panda 惡意程式樣態分析，分別為郵件樣本關聯分析與後門通聯流量分析。

●郵件樣本關聯分析

分析惡意郵件樣本，發現入侵方式區分為 4 個階段，詳見圖 9。




資料來源：本報告整理

圖9　郵件後門程式入侵方式

第一階段以捷徑檔方式啟動，產生誘餌文件與第一階段鏈結，第二階段則開啟誘餌文件，啟動 dropper，產生 downloader。Downloader 啟動後會連線至中繼站下載最終階段之後門程式並執行。

●後門通聯流量分析

分析網路攻擊之案件，其後門均是透過 Cobalt Strike 所產生。Cobalt Strike 是一套紅軍滲透測試工具，採 Client-Server 架構，可支援鍵盤側錄、檔案管理、提升權限、密碼擷取等功能。透過 Sever 端設定來產生對應之 Client 端後門，Server 端之設定檔為 Malleable C2 profile，可自行定義或直接從公開網路平台，如 github、技術論壇等，下載已設定好之範例，並用以定義 Client 端報到之類型與方式。

Client 端後門程式則是對應 Server 端之設定資料，包含協定、Port、網址、加密金鑰與傳送格式等欄位。

## 3.3 偵測與預警機制

Mustang Panda 發送以 COVID-19 為主題之社交工程郵件，藉由附件之惡意程式，入侵且操控受害電腦。除持續要求使用者提升資通安全意識外，藉由以下步驟及早偵測到機關是否已受害。

首先藉由分析中繼站通聯類型，受害者與中繼站間之通聯過程分為 3 種類型，首次報到類型為受害主機向中繼站報告，接續指令遞送類型為中繼站連線受害主機，最後結果回傳類型為受害主機回傳至中繼站。通訊內容均會先經過加密，再編碼後送出；而封裝亦分為 2 種類型，包含 HTTP 流量封裝與 DNS 流量封裝。

由於雙方通聯過程透過 HTTP 與 DNS 正常協定完成，偵測不易，建議可針對異常 DNS 流量進行觀察，例如內部有主機長時間、固定時間間隔送出大量 DNS query，且詢問之 DN 前綴是一長串看似亂碼的字串者，如圖 10，就有較高的機率是惡意程式所送出，可針對發出 query 的主機再做進一步的調查。


資料來源：本報告整理

圖10 DNS 報到流量示意圖

另一種方式則可透過部署駭客曾使用過之 DN 名單，配合 DNS-tunnel 活動進行偵測行動。該族群因慣於利用離地攻擊手法，再搭配無檔案式操作進行攻擊，因此樣本比對上相形困難，技服中心將持續嘗試取得相關情資與樣本進行深入研究分析，以利掌握該族群活動，並提供政府機關相關情資與因應之道。

# 4. 結論

本季具指標性案例為透過加拿大政府網站遭駭客竊取上萬用戶憑證，而個資外洩災情之所以慘重在於使用者慣用同樣之帳號與密碼，也造成憑證填充攻擊日益盛行。對使用者來說，使用公開網路服務更應提高資安警覺，對於資通系統管理者則應定期檢測網站之安全；另一起案例為駭客挾持 Tor 流量以竊取比特幣，由於洋蔥路由網路存在惡意出口節點，駭客成功藉由 SSL Strip 手法進行中間人攻擊取得網路傳輸資訊，再利用使用者存取 Bitcoin Mixer 服務時，竊取比特幣。因此，服務提供者是否能提供安全服務，如連線或內容之加密應是相關使用者在存取前應檢視之重點。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 52.39%)類型為主，排除綜合類型「其他」外，其次分別為「網頁攻擊」與「設備問題」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「憑證填充攻擊資安管理」、「開源網路或軟體資安管理」及「系統日誌資安管理」，提出資安防護建議。

資安專題分享主題為 DLL Side Loading 攻擊手法簡介，資安廠商揭露可利用微軟遠端桌面應用程式之 DLL Side Loading 漏洞，讓駭客執行遠端程式碼。因原廠現階段認為將在後續版本更新，表示風險持續存在。建議檢視應用程式所呼叫使用之 DLL 是否有合法簽章，以及檔案目錄是否存有與系統目錄中相同名稱之 DLL 檔案。

另外，資安技術研析主題為 Mustang Panda 族群追蹤與樣態分析，此族群以利用武漢肺炎為題，企圖攻擊台灣。經關聯分析該族群近期活動後，發現 2 波與台灣相關攻擊，本季針對 Mustang Panda 這 2 波攻擊之惡意程式與偵測方式進行研析與說明。

# 資安相關活動

本季行政院資通安全處辦理之資安相關活動，說明如下：

## ◆ 109 年第 1 次政府資通安全防護巡迴研討會

因應新冠肺炎疫情，109 年第 1 次政府資通安全防護巡迴研討會改線上課程辦理。本次課程主題，分別為資安威脅趨勢與案例分享、資通安全管理法施行情形說明及 GCB 推動與 VANS 機制說明。

本次資安威脅趨勢與案例分享，除分析全球資安威脅案例外，另特別針對物聯網威脅與供應鏈攻擊活動進行案例探討。隨著 5G 逐步進入商轉階段，IoT 市場不斷成長，入侵物聯網裝置將成為駭客攻擊跳板與牟利管道，另一威脅趨勢則因政府機關與企業組織使用第三方提供之雲端服務服務需求增加，亦助長服務廠商成為攻擊目標。第二個主題說明資通安全管理法施行情形，概述政府機關資通安全維護計畫之實施重點與完成度，完成度較低者多因人力資源之限制，包含資通安全推動小組與資安專責人力之設置與資安稽核推動辦理等事項。

最後在 GCB 推動與 VANS 機制說明，主要概述 GCB 推動時程，並明訂 109 年預定公告之 GCB 項目，包含 Microsoft office 2016 系列與 Apache HTTP Server 2.4。另一重點則為因應資通安全管理法施行細則所規範之機關應盤點資通系統與建立相關風險評估，發展出政府機關資安弱點通報(VANS)機制，以期結合資訊資產管理與弱點管理，掌握整體風險情勢。

## ◆ 109 年中央及地方政府資通安全長及資訊主管會議

109 年資通安全長及資訊主管會議於 8 月 7 日，假台大醫院國際會議中心辦理，主要議題為討論當前資安情勢與未來推動策略、資通安全管理法施行情形及強化事項。鑒於國際資安情勢日趨嚴峻，特別提及機關資安長扮演關鍵角色應負起督導之責，推動落實各項資安相關業務；同時善盡告知

提醒之責，主動向其首長說明內部資安業務之重要性及相關風險，以爭取所需之資安經費及資安人力。

議程最後則規劃綜合座談，討論政府機關資訊(安)業務委外安全管理精進規劃。除討論因應委外安全管理之具體安全作為外，亦就所提具敏感性或國安(含資安)疑慮之業務範疇，請機關配合後續檢討及擴大適用之作業。