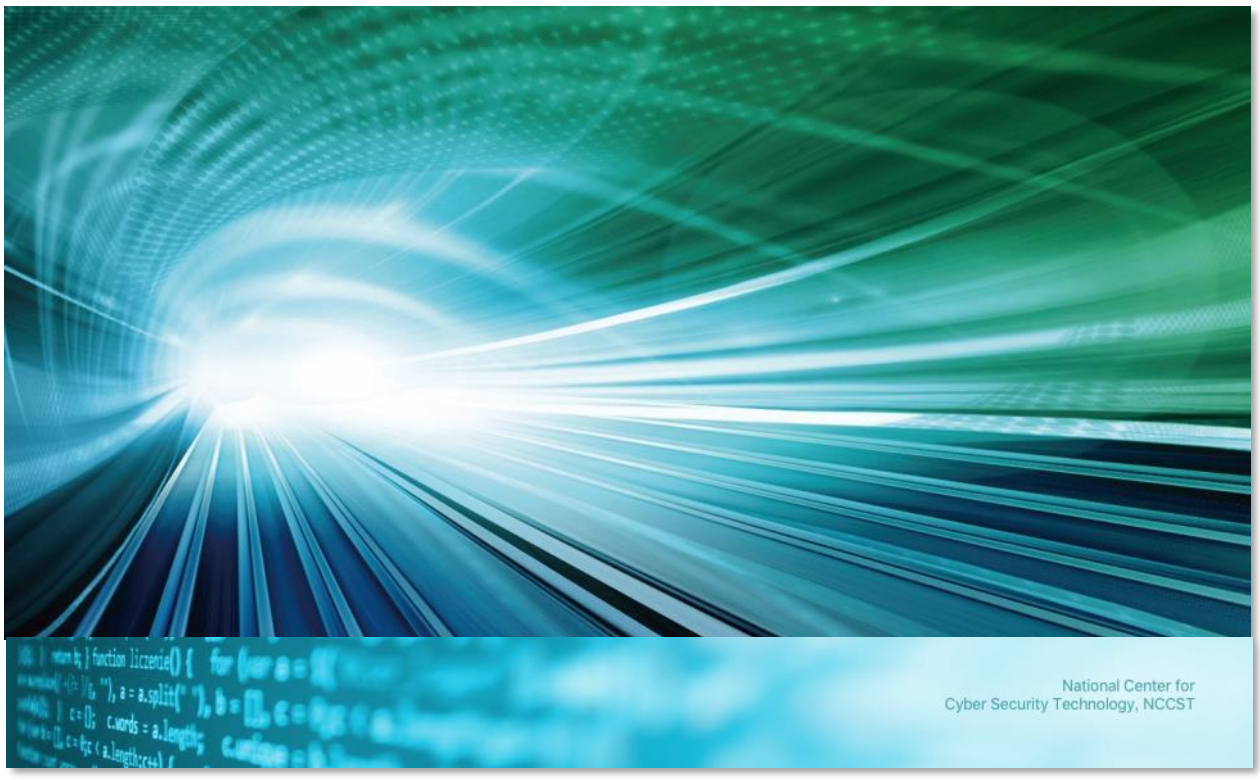
108年第2季資通安全技術報告

Quarterly Technical Report



目　次

圖 目 次

摘要

「第 2 季資通安全技術報告」除分析本季全球資安威脅、政府通報之資安事件外，並提供相對應之防護建議。同時，藉由資安專題之分享與資安技術之研析，提供政府機關(構)於資安風險的關注重點。

「第 2 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 起案例探討為國際與台灣之勒索病毒攻擊事件；另一起案例揭露台灣公共 DNS Quad101 遭 BGP 劫持。

分析政府資安威脅現況，發現政府機關(構)通報事件原因以「非法入侵」(占 39.58%)類型為主，「網頁攻擊」(占 24.6%)次之。

●2.資安專題分享

在資訊科技發展下，準備享受 5G 發展帶來之便利與應用的同時，針對資安或用戶隱私保護衍生出新的挑戰進行研析。正值 5G 相關技術與規範發展之萌芽階段，過渡期為 4G 與 5G 網路並存實現，應兼顧研析原有 4G 核心網路漏洞之解決方案，並持續觀測 5G 技術之安全提升。

●3.資安技術研析

由資安研究人員整理之資安技術研析，本季主題為攻擊者行為資料庫 MITRE ATT&CK(Adversarial Tactics, Techniques and Common Knowledge)與相關應用案例。攻擊者所使用的技術日新月異，藉著攻擊者行為資料庫 MITRE ATT&CK 的應用，可以讓組織了解自己應強化防禦技術之優先順序，透過不斷的進行攻擊演練測試，提升自我檢測能力，以成功防禦攻擊者可能之手法與技術。

●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，了解最新資安威脅現況與因應之防護重點。同時，資安專題分享 5G 相關技術與規範發展之萌芽階段，過渡期為 4G 與 5G 網路將並存實現，如何解決原有 4G 網路漏洞，並研析 5G 系統網路所面臨的資安問題與技術安全需求。此外，透過資安技術的研析，深入探討攻擊者行為資料庫所帶來之優勢與共通語言。在掌握本季之資安威脅現況時，亦說明下一季之資安專題重點，將探討無密碼時代之網路身分認證標準議題。

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。本季觀測到勒索軟體不僅在國外盛行，連同在國內也有遭勒索軟體入侵的事件發生，隨著勒索軟體技術發展漸臻成熟，伴隨著目標式攻擊的社交工程技巧，都是讓勒索軟體盛行不衰的原因。本章節的事件與議題皆配合整理相關之防護重點，提供組織就相關資安風險或議題進行評估，並依循防護重點進行強化。

1.1 全球資安威脅現況

研析全球網路攻擊事件，從早期駭客以分散式阻斷服務攻擊癱瘓網路運作，逐漸聚焦至進階持續威脅攻擊竊取機密資料。而隨著資訊科技運用與關鍵資訊基礎設施開放連網，物聯網設備資安弱點威脅升高與關鍵資訊基礎設施資安風險亦有倍增趨勢。另外，駭客成功駭進資安(訊)供應商，破壞整體供應鏈安全的事件更是時有所聞。除上述這些廣為人知的資安威脅外，包括國內外持續發生的資料外洩事件，這些外洩資料內的電子郵件地址、帳號密碼可能會持續發酵，越來越盛行的憑證填充攻擊(credential stuffing attacks)利用這些在網路上流傳的資料，進而在不同的網路服務或社群媒體上試圖登入。因此看似單一的資料外洩事件，造成的後續衝擊與後果仍有待受害組織持續觀測與注意。

第 2 季(以下簡稱本季)具指標性的案例為勒索病毒攻擊事件風行再起；另一起案例為台灣公共 DNS Quad101 遭 BGP 劫持。

首先，探討案例為勒索病毒攻擊事件。美國佛羅里達州(Florida)只有 3.4 萬居民的小城市 Riviera Beach 於 108 年 5 月 29 日感染勒索軟體，市議會於 6 月 19 日投票表決，決定支付 65 個比特幣(約 63 萬美元)贖金予駭客。此一意外源自於一名 Riviera Beach 市政府員工開啟電子郵件中所夾帶的惡意檔案，勒索軟體加密該市電腦系統重要檔案，造成該市電子郵件系統完全

無法使用，911 的調度員無法將來電輸入電腦系統，連支付薪水給員工或承包商都只能開支票，而無法透過電腦轉帳。

佛州另一個只有 1.2 萬名居民的小城市 Lake City 則於 108 年 6 月 10 日遭到勒索軟體攻擊，勒索軟體加密 Lake City 系統重要檔案，使得電子郵件系統、多數市內電話及其它網路服務都無法運作，只有提供警方及火災等公共安全的網路，因隔離而未受波及。市議會於 6 月 24 日召開緊急會議，也決定支付駭客所要求的 42 個比特幣(約 50 萬美元)贖金。成為繼 Riviera Beach 之後，第二個支付勒索贖金的佛羅里達州城市。

在國內亦發生相關勒索病毒攻擊事件，基隆市政府全球資訊網 108 年 5 月 4 日傳出被勒索病毒入侵，系統癱瘓 3 天，至今外部網路民眾已可上網，但內部網路仍未恢復，多名議員擔心資安恐出現問題，機密資料、民眾個資是否外洩。市政府研考處澄清市民個資未外洩，僅內部作業系統受影響。

第 2 起案例為台灣公共 DNS Quad101 邊界閘道器協定(Border Gateway Protocol，以下簡稱 BGP)遭劫持。Quad101 是一實驗性的公共 DNS，由台灣網路資訊中心(TWNIC)營運，推廣以隱私為主的 DNS 服務。108 年 5 月 8 日，DNS Quad101 遭到劫持，封包持續被導向巴西一家網路業者(ISP)，所幸持續時間僅三分半鐘，並未造成太大影響。

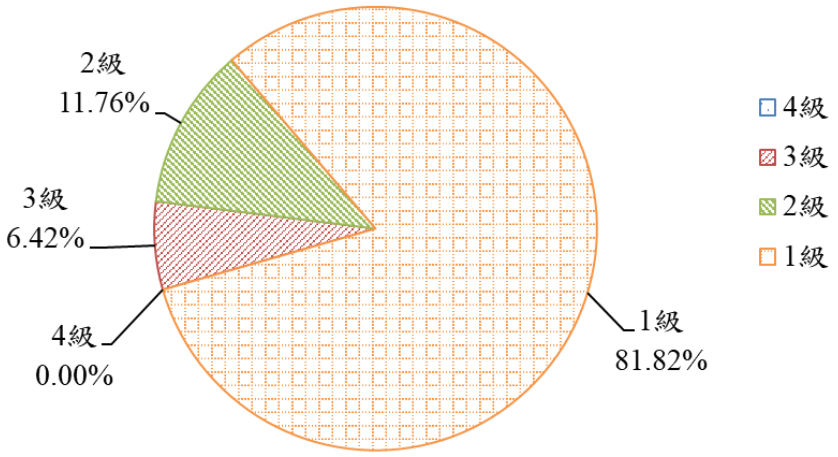
去年全球亦發生類似 BGP 遭劫持之資安事件，由甲骨文(Oracle) Dyn 網路分析總監 Doug Madory，於 107 年 8 月 3 日揭露另一起 BGP 挾劫持攻擊，指出駭客先入侵了位於印尼及馬來西亞的兩家 ISP 業者，散布錯誤的路由資訊，以將美國三大支付業者的流量導至駭客所控制的伺服器。駭客集團於 107 年 7 月藉由入侵印尼 Digital Wireless 與馬來西亞 Extreme Broadband 兩大 ISP 業者，竄改 Datawire、Vantiv 及 Mercury Payment Systems 三大支付業者的路由，讓假冒的 DNS 伺服器能夠傳遞偽造的回應，把原本要造

訪這三大支付業者的使用者導至惡意網站。此外，駭客還在偽造的回應中採用更長的存活期(Time to Live，以下簡稱 TTL)，讓這些假冒的 DNS 可在遞迴 DNS 伺服器中保留到 BGP 挾持結束為止，以最大化攻擊時間。一般網域的 TTL 為 10 分鐘，但在此次的攻擊中，駭客把偽造回應的存活期最高設為 5 天，目的是為了能有更充裕的時間竊取支付卡業者的客戶資訊。在展開攻擊的這幾天，使用者經常抱怨無法連上官網。

綜覽本季重大資安事件，駭客鎖定政府機關發動勒索軟體攻擊，企圖影響公共資通系統服務，造成社會與民眾不安，進而達成勒索目的。同時因為美國兩個城市支付勒索贖金的作法，也會鼓勵駭客鎖定那些高度電腦科技化，卻缺乏相對應資安基礎設施的小型城市展開攻擊；而 BGP 遭劫持之資安事件也顯示網路基礎設施的脆弱與日常維運管理的重要性。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關(構)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(構)之資安威脅現況。通報事件依資安事件對「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級資安事件。彙整事件影響等級，本季以 1 級事件占 81.82%為大宗，2 級事件占 11.76%次之，3 級事件僅占 6.42%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

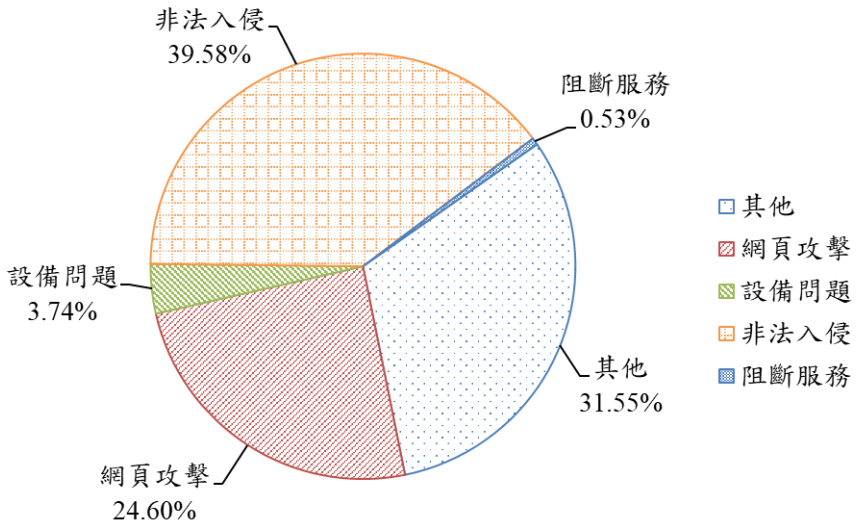


資料來源：本報告整理

圖1　108 年第 2 季資安事件影響等級比率圖

本季 3 級重要資安事件主要為攻防演練通報案件占比居多，多數機關評估在攻擊團隊成功入侵受測目標後，可造成敏感資料遭洩漏，因此通報為 3 級事件。另外，舊公文系統之資料遭竊，造成大量公務人員資料外洩案例亦列為 3 級重要資安事件。

此外，資安事件通報類型依其所發現之異常情形，包括非法入侵、網頁攻擊、設備問題、阻斷服務及其他，其中，以「非法入侵」(占 39.58%)類型為主，大部分為伺服器遭入侵後，被植入惡意程式並向中繼站進行連線行為，詳見圖 2。



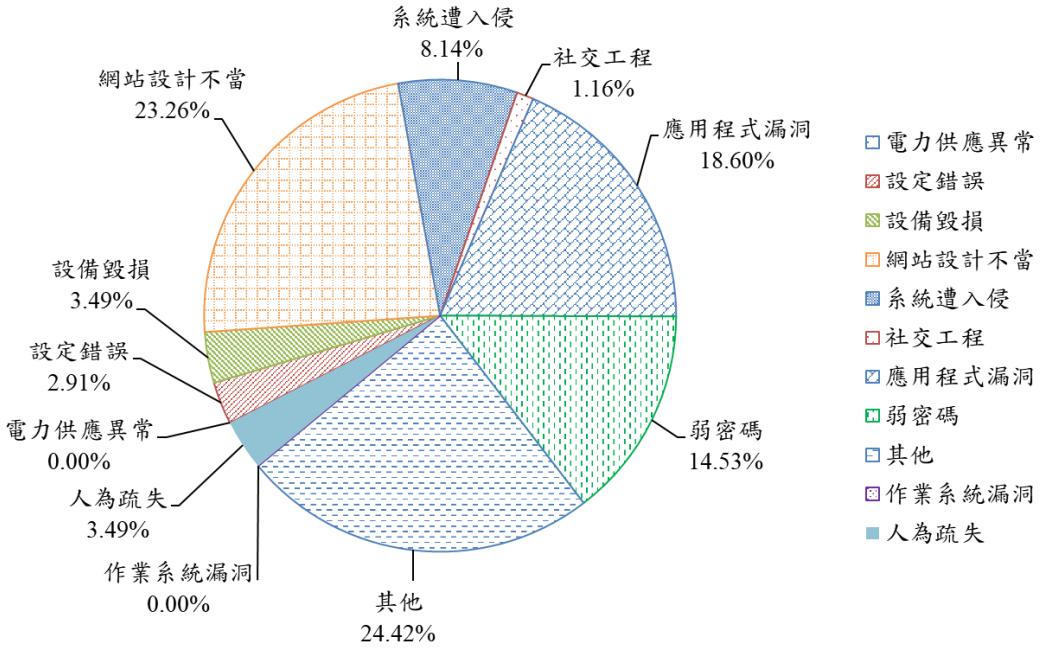
資料來源：本報告整理

圖2　108 年第 2 季資安事件通報類型比率圖

最後，分析通報事件發生原因，以其他(占 24.42%)為主，其次分別為網站設計不當(23.26%)、應用程式漏洞(18.60%)、弱密碼(14.53%)、系統遭入侵(8.14%)、人為疏失(3.49 %)、設備毀損(3.49 %)、設定錯誤(2.91%)、社交工程(1.16%)、作業系統漏洞(0.00%)及電力供應異常(0.00%)，詳見圖 3。本季事件之其他(占 24.42%)高的原因，除 28 件為攻防演練機關判定為事件原因列為其他外，因本季發生華碩網路硬碟服務遭中間人攻擊散布後門程式影響，在部分機關使用華碩雲端服務程式，卻在更新雲端服務程式時下載惡意程式，此類事件歸因為其他。同時，部分機關因人力、資源不足或紀錄遭駭客刪除，無相關日誌紀錄可進行事件調查，或無直接證據說明遭入侵管道，亦以事件原因不明進行結報，先暫列為其他。

上述事件發生肇因部分是由於委外廠商或外部供應商遭入侵進而影響通報機關，如維護廠商提供予機關之資訊設備未落實適當的檢查與管制，導致存有惡意程式之資訊設備利用機關網路進行中繼站連線；或委外廠商遭感染勒索軟體並透過遠端存取擴散至通報機關；亦或是利用應用程式更新機

制入侵通報機關。



資料來源：本報告整理

圖3　108 年第 2 季資安事件原因比率圖

1.3 資安防護重點

分析本季全球資安威脅現況，美國數個城市與台灣發生之勒索病毒攻擊事件，在現行社會環境高度使用資通訊科技，對部分地方政府或小型城市在資安防護資源不足情況下，更加容易成為駭客鎖定對象。BGP 遭劫持之資安事件頻傳，若無法即早發現，可能造成財務損失或其他重大影響。

分析政府機關(構)通報的 3 級資安事件可看出，個人資料或機敏性資料依然是駭客的首選目標。另外，因為未針對委外廠商進行適切的監督管理機制，促使機關間接成為受害者，都顯示委外管理尚有加強空間。

綜整以上資安威脅現況，提供資安防護建議如下：

●委外管理

– 依循「資通安全管理法」規定委外辦理資通系統之建置、維運或資通服務之提供，選任適當之受託者；委任前應先檢視是否具備完善之資通安全管理措施或通過第三方驗證。

– 確認委外廠商之人員能量與資歷，是否配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

– 檢視委外廠商之資通安全維護措施，並定期監督其資通安全維護情形。

– 簽訂服務水準協議，並要求委外廠商知悉資通安全事件時，應立即通報並採行適當之補救措施。

●勒索軟體防範

– 強化內部人員資安意識，對資安風險維持高度警覺。

– 區分資料重要性後，依優先性規劃與定期進行離線與異地備份。

– 依據最小權限原則訂定存取限制，並建立軟體安裝的存取控制規則，對未知程序進行管制。

●BGP 組態安全管理

– IP 段位址字首過濾，設定只在必要時接受 IP 段位址字首聲明，並且只應將其 IP 位址字首指定到特定網路。

– 主要的 DNS 服務供應商以 RPKI (Resource Public Key Infrastructure)來簽署路由，RPKI 基於公共密鑰基礎建設框架，用於保護網際網路路由基礎建設，並以 EBGP (External BGP)來驗證路由，可以減少路由劫持與其他攻擊事件。

– 定期監控網路流量與日誌，設定正常基準線，並定義警示值。

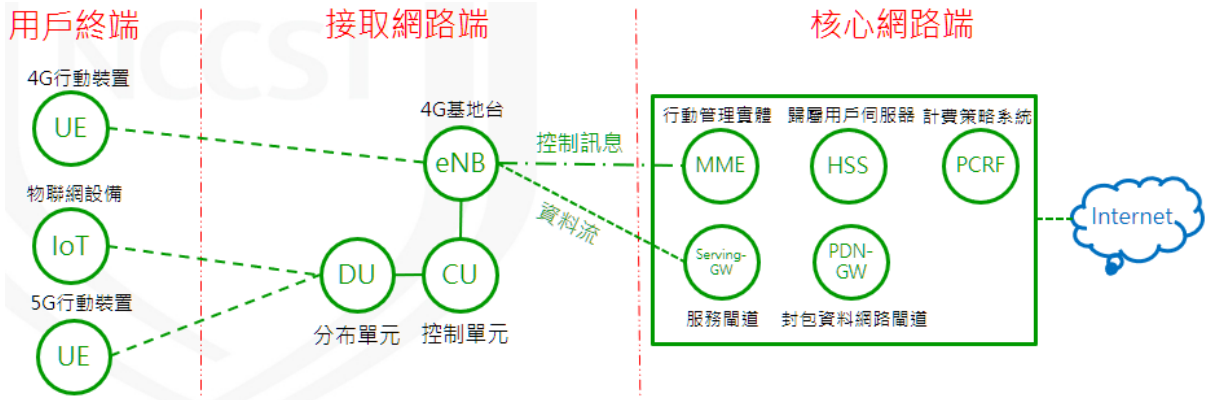
2. 資安專題分享

長久以來，許多服務與應用受限於 4G 速度與穩定性，而無法嶄露頭角進而普及大眾，也因近年來智慧應用的發達，如智慧型手機、無人載具及人工智慧等，致使大眾對頻寬的需求與日俱增。因此當 5G 逐漸發展的同時，許多需要更快下載速度的服務與應用也會迅速增長。尤其是在物聯網逐漸普及的應用上，5G 的行動通訊技術勢必帶來科技服務嶄新的應用層面。

而在各界啟動對下一代行動通訊技術 5G 的研究，並在提升行動網路用戶服務體驗的基礎上發展新服務、新架構及新技術，同時亦會對資安或用戶隱私保護衍生出新的挑戰。由於目前正值 5G 相關技術與規範發展之萌芽階段，此過渡期 4G 與 5G 網路將並存實現，因此研析 5G 系統網路所面臨的資安問題與需求時，亦應兼顧研析原有 4G 運作網路漏洞之解決方案，並持續觀測 5G 技術之安全提升。

2.1 5G 網路架構背景說明

為提供更進一步之高畫質影音與高速寬頻服務， 5G 初步以強化無線接取技術為主，核心網路初期主要仍沿用 4G 核心網路架構，接取網路則導入無線接取分離架構(包括控制單元(CU)與分布單元(DU) 2 個實體)，以實現 5G 低延遲與高流通量的特性，用戶終端部分主要為同時具備 4G 及 5G 信號接收的行動裝置(User Equipment，以下簡稱 UE)或物聯網裝置，詳見圖 4。



資料來源：本報告整理

圖4　4G 與 5G 網路並存網路架構

在用戶終端的 UE 中，有許多重要的資訊，包括用戶識別模組(Subscriber Identity Module，以下簡稱 SIM)、國際行動用戶識別碼(International Mobile Subscriber Identity，以下簡稱 IMSI)及國際行動裝置識別碼(International Mobile Equipment Identity，以下簡稱 IMEI)。SIM 是用於儲存用戶的識別碼、認證方法及密鑰，可供電信網路對用戶身分進行認證，同時用戶也能通過 SIM 完成與電信網路的連接與訊息的交換；IMSI 為用戶之獨特 ID，通常會寫入 SIM 卡中；IMEI 則為手機之獨特識別碼，類似 MAC address。為保護用戶 IMSI 識別碼的隱私問題，電信網路採用「臨時行動用戶識別碼(Temporary Mobile Subscriber Identity，以下簡稱 TMSI)」來做為認證後用戶身分的臨時識別，並會隨時間及用戶所在位置更動而變換。

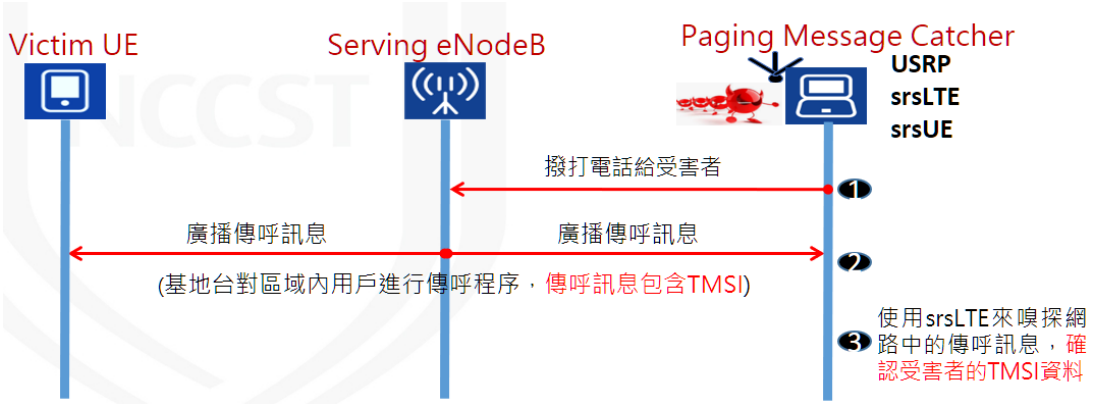
根據 108 年 2 月普渡大學與愛荷華大學研究人員最新之研究分析，針對目前的 4G 網路架構提出藉由傳呼通道(Paging Channel)攻擊，可以成功取得特定用戶之 TMSI 與 IMSI 敏感資訊。一旦用戶之 TMSI 與 IMSI 遭鎖定，則可能引發用戶地理位置洩漏或發送惡意廣播訊息等安全議題，由於在目前的規範中，5G 網路仍沿用 4G 的傳呼通道技術，因此也連帶影響即將推出的 5G 網路隱私安全，以下將概述傳呼通道攻擊手法。

2.2 傳呼通道攻擊手法研析

傳呼(Paging)是當有通話或簡訊服務時，核心網路端要確認 UE 的位置與狀況，就必須透過基地台廣播傳呼訊息(Paging Message)，完成尋找 UE 之目的。而攻擊者則是利用傳呼協議的漏洞，來取得 TMSI 與 IMSI 敏感資訊。以下說明攻擊者利用的 3 種攻擊方式。第 1 種攻擊是 ToRPEDO，攻擊者可透過分析傳呼訊息來取得用戶的 TMSI，進而追蹤用戶的所在位置，甚至劫持傳呼通道，取得用戶隱私訊息，而另外 2 種進階式攻擊為 PIERCER 與 IMSI-Cracking，攻擊者可以基於 ToRPEDO 的攻擊手法，進一步破解國際行動用戶識別碼(IMSI)。

●ToRPEDO

ToRPEDO (TRacking via Paging mEssage DistributiOn)攻擊手法是攻擊者利用當有電話或訊息傳到閒置的手機前，核心網路端會透過當地基地台(Serving eNodeB)，廣播發出內含 TMSI 傳呼訊息的特性來進行攻擊。首先，攻擊者須事先得知受害者(Victim UE)的電話號碼，並架設攻擊平台以擷取訊息(包括 USRP B210(無線射頻收發模組)硬體設備與 srsUE(模擬手機)與 srsLTE(無線協議分析)軟體)。接著，攻擊者在短期間內接連撥打多次電話給受害者又迅速掛掉，來啟動核心網路發送傳呼訊息，藉由嗅探這些傳呼訊息，不超過 10 通撥打電話就能確認用戶 TMSI，攻擊流程詳見圖 5。

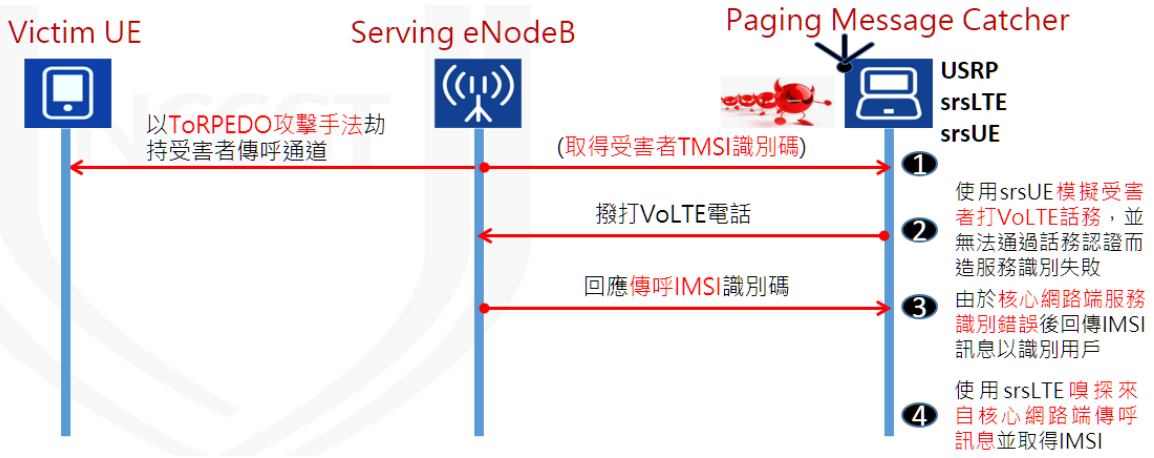


資料來源：本報告整理

圖5　ToRPEDO 攻擊流程

●PIERCER

PIERCER(Persistent Information ExposuRe by the CorE netwoRk)攻擊主要是藉由 ToRPEDO 攻擊所取得的受害者 TMSI，使用 srsUE 偽裝受害者手機撥打 VoLTE 電話，由於攻擊者無申請 VoLTE 服務功能而造成 VoLTE 話務的認證失敗，依目前 3GPP (3rd Generation Partnership Project)之規範，當用戶終端傳送的 TMSI 訊息服務是無效且核心網路端無法識別時，核心網路端將會嘗試傳呼 IMSI 來確認用戶是否為有效用戶，攻擊者即可藉由核心網路端所回應的傳呼訊息來取得受害者的 IMSI，攻擊流程詳見圖 6。



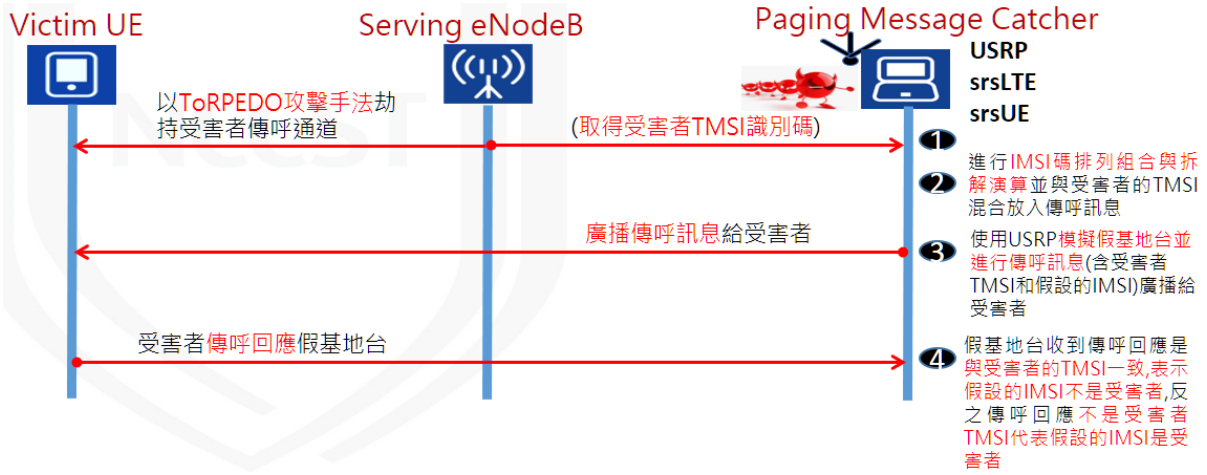
資料來源：本報告整理

圖6　PIERCER 攻擊流程

●IMSI-Cracking

IMSI-Cracking 之攻擊手法是攻擊者偽裝成假基地台，發送傳呼訊息給受害者，並在傳呼訊息中放入 ToRPEDO 攻擊所取得的受害者 TMSI，以及利用亂數方式產生的 MSIN。依現行的系統設定，用戶 UE 若接收到內含 IMSI 與 TMSI 的傳呼訊息，將優先以 IMSI 身分處理並回應核心網路端，若非受害者的 IMSI，則以 TMSI 身分進行回應，攻擊者即可利用此

特性來確認猜測的 IMSI 是否與受害者一致，並進一步取得受害者 IMSI，攻擊流程詳見圖 7。



資料來源：本報告整理

圖7　IMSI-Cracking 攻擊流程

2.3 5G 網路之衝擊與防護建議

分析 5G 系統網路資安威脅，威脅來源分別可從用戶終端、接取網路端及核心網路端展開，舉例來說，用戶終端可能達遭受降階攻擊與惡意程式攻擊；在接取網路端則可能面臨監聽攻擊與訊息重送攻擊及核心網路端之網路切片、虛擬化環境及流量攻擊等資安威脅。

現階段國際標準組織 3GPP (3rd Generation Partnership Project)，正在制定 5G 安全標準與相關安全要求。而目前 3GPP 標準雖針對以 IMSI 誘捕設備(假基地台)來取得用戶 IMSI 識別碼隱私問題，已要求使用公私鑰機制來進行 IMSI 識別碼的保護，以解決用戶端的安全隱私洩漏，但對於本報告所提出之傳呼通道攻擊手法，尚未有安全防護要求，用戶隱私洩漏問題依然存在。再加上目前的規範 5G 網路仍沿用 4G 的傳呼通道技術，因此攻擊者也能使用上述 3 種攻擊手法於 5G 網路的傳呼通道，以取得用戶敏感資訊。

因此除透過 3GPP 標準組織之安全規範與要求外，因應新興行動通訊技術的崛起，現有的資安防禦措施更需持續不斷地精進，因此研析新興網路資安技術來抵禦相關網路威脅，並提升自身資通安全防護能量，已然是當務之急。隨著 5G 應用發展，面臨可能之威脅來源，5G 業者可具體規劃與推動新興網路安全技術，透過網路功能虛擬化(Network Functions Virtualization, NFV)與軟體定義網路(Software Defined Networking, SDN)2 大網路革新之關鍵技術，先加強基礎網路技術之安全，藉以提升網路資源的使用效率、降低網路營運的成本，同時又可滿足創新網路應用的需求。

5G 網路商業化即將來臨，而傳呼通道技術雖為成熟技術，但其所隱藏之安全隱憂亦不容輕忽，因此在國際規範尚未更新安全要求或制定出新的標準前，提供以下 5G 網路基礎防護建議：

- 建議經常更新 TMSI 識別碼，以避免 TMSI 識別碼被鎖定利用。
- 建議使用公私鑰機制加密，以保護無線傳呼訊息。
- 建議電信業者基地台部署憑證進行認證，以防止假基地台問題。
- 建立測試平台模擬攻擊與實作時可能面臨之資安威脅，逐步提升自身資通安全防護能量。

3. 資安技術研析

本季所探討的資安技術研析，是概述攻擊者行為資料庫 MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge)與相關應用案例。攻擊者所使用的技術日新月異，隨著社群網路的發達，各式各樣的攻擊手法與技術也藉著社群網路擴散並相互學習。因此如何知己知彼，藉著攻擊者行為資料庫 MITRE ATT&CK 的應用，可以讓組織了解自己應強化防禦技術之優先順序，透過不斷的進行攻擊演練測試，提升自我檢測能力，以成功防禦攻擊者可能之手法與技術。

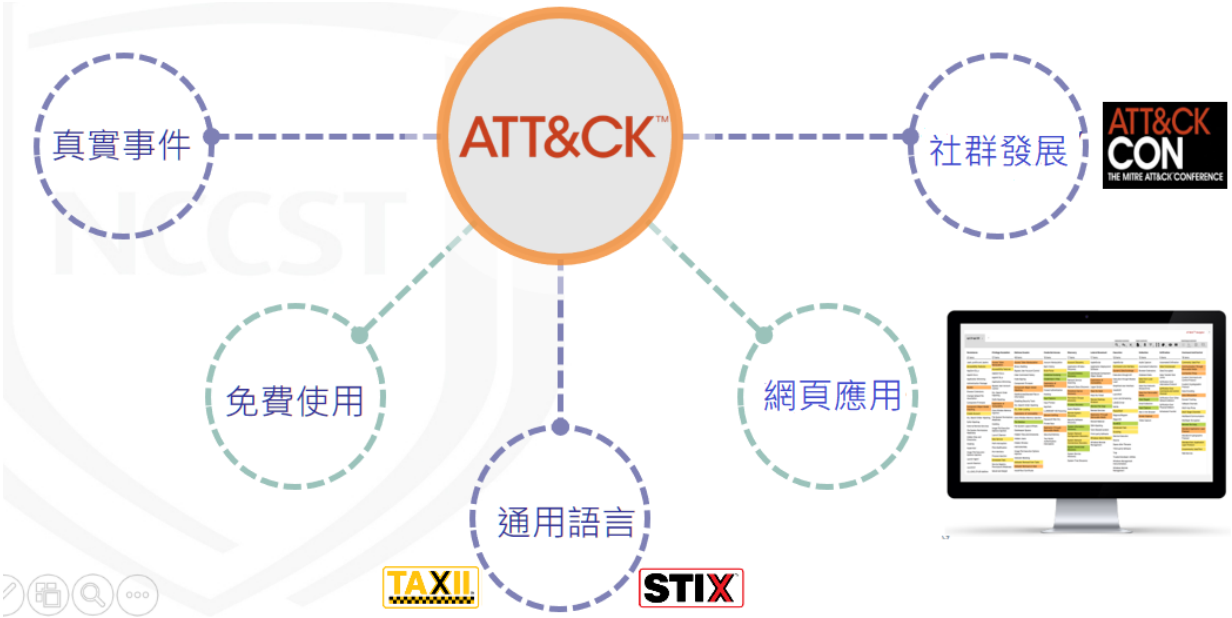
3.1 攻擊者行為資料庫 MITRE ATT&CK 概述

MITRE 是一家美國非營利組織，除協助進行多項資安相關研究，同時，也是維運 CVE 漏洞資料庫背後的組織，相關網路安全的重要研究成果，包括「資安弱點情資分享」，管理 CVE 網站、CWE 網站及 CAPEC 網站、「資安威脅情資分享」，例如推動自動化威脅情資交換機制與攻擊者行為資料庫 ATT&CK、「開發開源資安工具」，則有 Cuckoo 與 Yaraprocessor 工具及「資安技術文件」，如資安情資、資安趨勢預測及軟體開發安全等。

MITRE 於 104 年 5 月發起 ATT&CK 框架的研究計畫，主要是希望建立一個可供全球自由運用，基於真實世界所觀測到之對手戰術與技術的知識庫。ATT&CK 知識庫可被運用在開發政府、企業及網路各項安全產品與服務中之特定威脅模型與方法的基礎。ATT&CK 針對攻擊流程的定義，提出更具系統性的歸納，藉由建立簡單易懂的模型與通用語言，如此一來，可以讓各家資安業者在說明網路攻擊方法時，有統一的標準去依循。對於政府機關與企業則可以透過這樣的工具，更方便地理解攻擊者行為帶來的資安風險。

彙整與分析網路威脅情資，才能真實面對最新的網路威脅。MITRE

ATT&CK 基於建立與描述攻擊者行為的知識庫，對駭客入侵策略所採用的各式技術手法，都有詳細介紹，不僅提供真實事件會運用之攻擊手法，還有駭客集團使用手法，且有減緩與偵測之相關說明，ATT&CK 框架詳見圖 8。



資料來源：本報告整理

圖8　ATT & CK 框架

從此框架可看出 ATT&CK 的整體應用，最主要藉由模擬真實事件中駭客攻擊情境，以識別並進而了解相關攻擊手法。透過免費的共享資源協助各界溝通入侵事件，並為組織內部之防禦評估與攻防演練，提供理解攻擊者具備能力之知識庫。另外，在通用語言方面，提供 2 種不同的介接工具 STIX 2.0 GitHub repository 與 TAXII Server，以連結 ATT&CK。再以網頁應用程式為例，其介面風格類似 Excel 試算表，讓用戶應用 ATT&CK 矩陣可以更加便利，此線上服務具備對應 Windows、Linux 與 Mac 平台的篩選器，讓用戶能直覺的檢視自身的防禦範圍，並能將結果匯出成向量圖檔或

XLSX 檔。最後，基於網路資源共享並透過社群發展、論文發表及辦理 ATT&CK 大會，以持續推廣與改進 ATT&CK 框架。

ATT&CK 依戰術(Tactics)與技術(Techniques)分為 3 大部分，包括 ATT&CK Enterprise、Pre-ATT&CK 及 ATT&CK for Mobile。ATT&CK Enterprise 描述具體的攻擊入侵過程，其技術細節涵蓋 Windows、Mac 及 Linux 系統平台；Pre-ATT&CK 則為對應攻擊前準備，另外，ATT&CK for Mobile 則是針對現行應用廣泛的行動裝置，所發展出來的框架。

3.2 MITRE ATT&CK 運作框架與方式

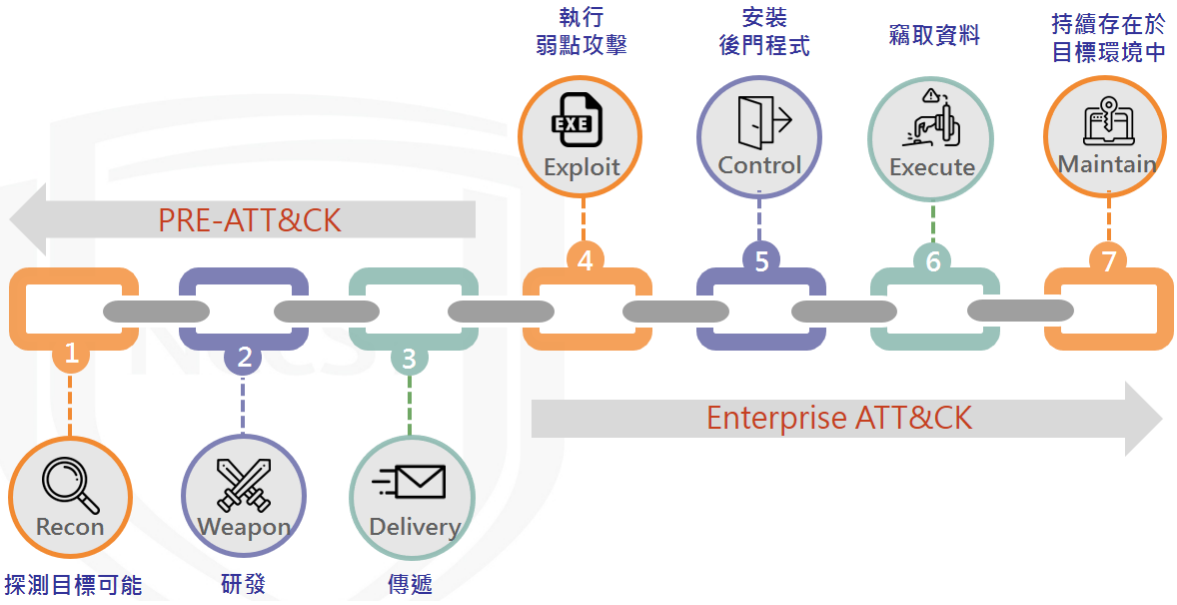
現今威脅趨勢有越來越多的敏捷式攻擊者，未來的攻擊者將會更靈活及更具變化性。敏捷式的攻擊手法有幾項特徵，除持續利用新漏洞與工具外，代表攻擊者之攻擊元件將更能適應在不同的目標環境，而且攻擊者入侵後會藏匿於合法的使用者行為中，包括使用合法的元件、濫用合法使用者憑證、仿冒合法使用者行為等。因此，如何建立基於風險而產生之威脅模型，針對敏捷式攻擊者進行分析，從深刻了解內部脆弱、威脅及相關衝擊，建議從以下 3 個步驟進行防禦準備。

首先，確認組織關鍵業務與資產，分析會有那些攻擊者及為何攻擊者會對這些資產感興趣。接續，透過威脅情資了解攻擊者的攻擊元件，透過如入侵指標 Indicators of Compromise(IOC)、產品分析報告 Certificate of Analysis(COA)等情蒐文件驗證。最後觀察攻擊者的戰術、技術及流程 Techniques, Tactics and Procedures(TTP)。整個防禦過程中最關鍵的步驟，則是可運用 ATT&CK 對攻擊者的 TTP 進行檢測、防禦及應變。

ATT&CK 著重於網路威脅情資的資料庫蒐集，透過 MITRE ATT&CK 的框架，就能快速描述攻擊者如何準備、發起及執行攻擊。此外，MITRE ATT&CK 框架也能結合目前最常被使用的「網路攻擊鏈(Cyber Kill Chain)」，MITRE ATT&CK 將攻擊流程的定義，做出更具系統性的歸

納，可以讓入侵手法描述有一致性標準，成為簡單易懂的模型與通用語言。如此一來，各家資安業者在說明網路攻擊鏈時，有統一的標準去依循，而組織亦可透過此工具，更方便地理解攻擊者行為帶來的安全風險。

網路攻擊鏈結合 ATT&CK 框架，可以觀測駭客的 Pre-ATT&CK，是從初始階段運用具目標式或盲目式的探索可入侵之目標，揭露資通系統或防護上之漏洞，研發相關工具或手法，互相傳遞攻擊訊息。當駭客完成攻擊前準備，就會進入 ATT&CK Enterprise 階段，針對目標對象解析弱點並展開攻擊，進而安裝後門程式，藉機竊取機敏性業務資料，甚至達到不被入侵對象發現而持續潛伏存在於目標環境中，詳見圖 9。



資料來源：本報告整理

圖9　網路攻擊鏈模式

ATT&CK 針對最主要的 Enterprise 提供矩陣(Matrix)供外界參考，詳見圖 10。藉由 Enterprise Matrix，橫軸代表戰術(Tactics)，表示攻擊者的目標，而縱軸代表技術(Techniques)，表示攻擊者達成目標的方式。

戰術 ⟶

技術 ↓

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destructio
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacemer
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Conte Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruptio
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery

資料來源：https://attack.mitre.org/matrices/enterprise/

圖10 ATT&CK Enterprise Matrix

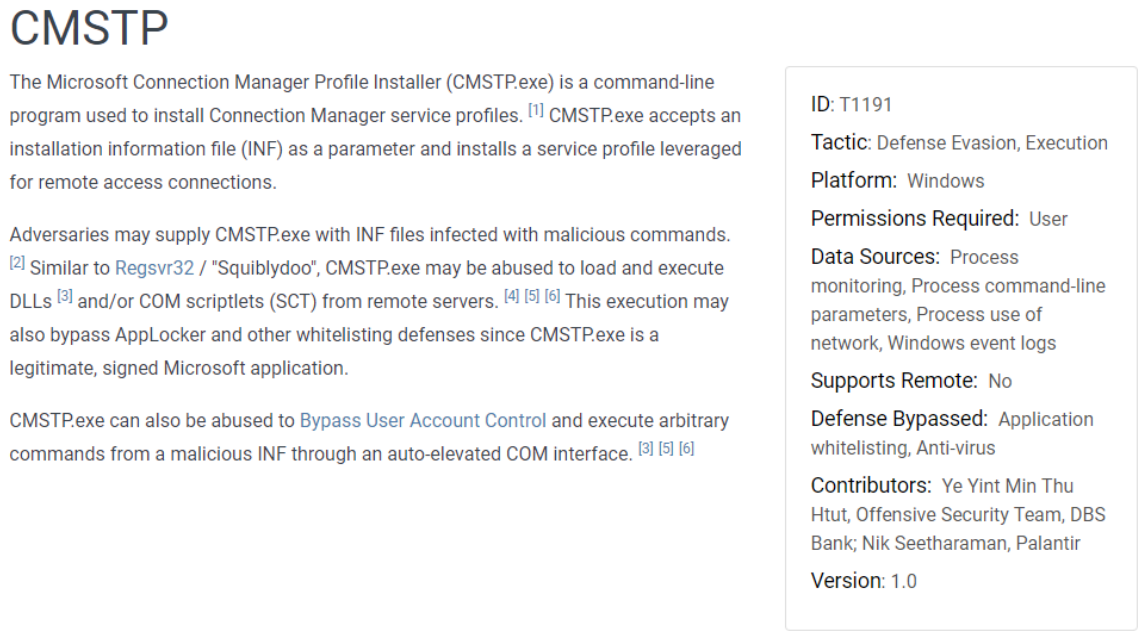
3.3 MITRE ATT&CK 應用案例

運用 ATT&CK 有助於管理者預知與理解已知攻擊者行為可能帶來的資安風險，以資安業者或組織角度來看，都可以藉此改進他們的檢測與預防方法。如對於企業而言，能幫助評估與選擇適合的工具，以改善其網路防禦。以 4 個階段來進行檢測、模仿攻擊、威脅情資及防禦等階段性防護進行機制設計，如優先關注對組織具威脅的攻擊手法，以考量相應的資安措施。

以微軟 CMSTP 為例，CMSTP.exe 是用於安裝或刪除 Connection Manager 服務配置文件的程序，可接受 INF 文件作為參數，是一個合法、已簽名的 Microsoft 應用程序。但攻擊者可以藉由向 CMSTP.exe 提供感染惡意命令的 INF 文件，從遠程服務器加載與執行 DLL 或 COM scriptlet(SCT)等。此種攻擊方式還可以繞過 AppLocker 與其他白名單防禦。另外，CMSTP.exe 亦可被濫用來繞過用戶帳戶控管機制，並通過自動提升的 COM 存取點從

惡意 INF 執行任意命令。

組織可從 ATT&CK 資料庫中了解有關 CMSTP 的技術細節，了解駭客如何利用 CMSTP 繞過配置不佳的應用程序白名單列表，以及如何通過 WebDAV 獲得提權的 shell 或遠程下載任意代碼，詳見圖 11。



CMSTP

The Microsoft Connection Manager Profile Installer (CMSTP.exe) is a command-line program used to install Connection Manager service profiles. [1] CMSTP.exe accepts an installation information file (INF) as a parameter and installs a service profile leveraged for remote access connections.

Adversaries may supply CMSTP.exe with INF files infected with malicious commands. [2] Similar to Regsvr32 / "Squiblydoo", CMSTP.exe may be abused to load and execute DLLs [3] and/or COM scriptlets (SCT) from remote servers. [4] [5] [6] This execution may also bypass AppLocker and other whitelisting defenses since CMSTP.exe is a legitimate, signed Microsoft application.

CMSTP.exe can also be abused to Bypass User Account Control and execute arbitrary commands from a malicious INF through an auto-elevated COM interface. [3] [5] [6]

ID: T1191

Tactic: Defense Evasion, Execution

Platform: Windows

Permissions Required: User

Data Sources: Process monitoring, Process command-line parameters, Process use of network, Windows event logs

Supports Remote: No

Defense Bypassed: Application whitelisting, Anti-virus

Contributors: Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank; Nik Seetharaman, Palantir

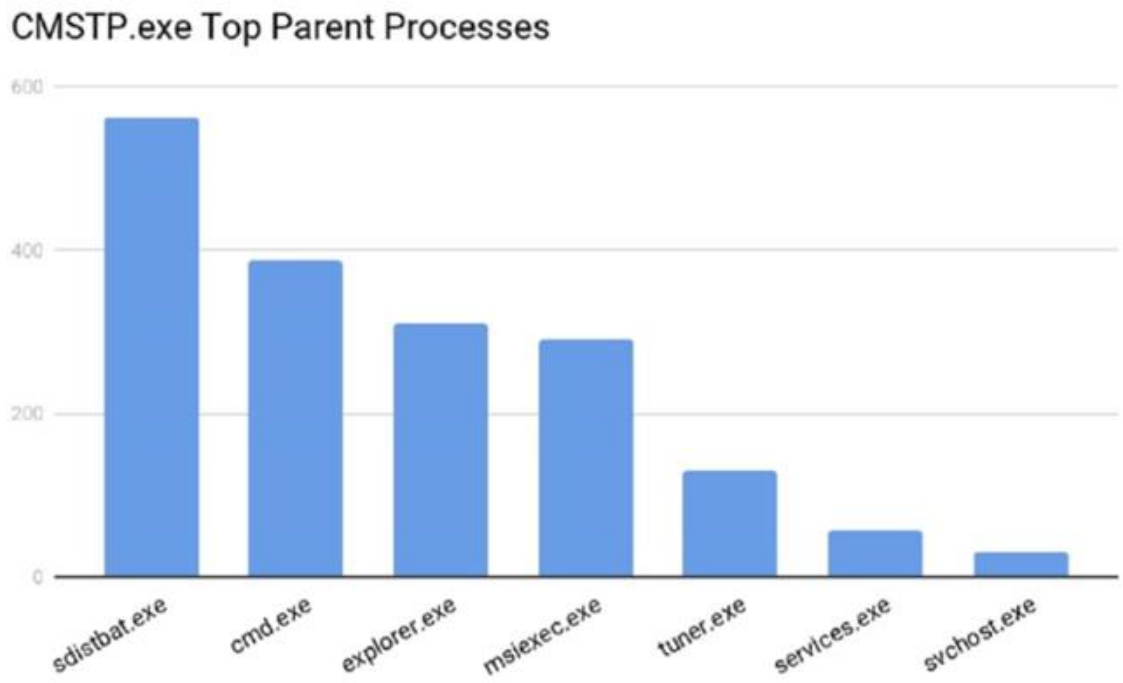
Version: 1.0

資料來源：https://attack.mitre.org/techniques/T1191/

圖11 CMSTP 技術說明

ATT&CK 資料庫除提供 CMSTP 上述攻擊手法範例外，亦提供減緩攻擊的組態設定方式，包括 CMSTP 在既有環境中可能沒有必要啟動，除非使用 VPN 連接或是考慮使用配置為阻止 CMSTP.exe 執行之應用程序白名單，以防止惡意者濫用。

ATT&CK 就偵測面提供管理者可從以下幾點，進行威脅的分析與了解，如了解程序是否經過簽名、程序是否能執行遠端指令及父程序(Parent Process)調用 CMSTP 的頻率等，來分析相關攻擊的活動可能性，詳見圖 12。



資料來源：本報告整理

圖12 CMSTP 父程序執行頻率排名

整體而言，MITRE 提出的 ATT&CK 資安框架，使威脅入侵的描述具有一致性標準，運用其基礎知識庫，協助組織更加理解攻擊者的行為模式，相對亦能為內部攻防演練帶來助益。

在安全維運面，學習如何使用 ATT&CK 強化網路安全技術，關注在政府機關或企業如何透過 ATT&CK 強化自身網路安全技術，模擬攻擊者之行為，以預先規劃風險回應之優先順序，進而採取相對應之風險處理計畫。在人員部分，藉此訓練員工了解與強化專業知識；在流程方面，研發或創新防禦技術時可參考 ATT&CK 之框架；在威脅情資部分，則可透過 ATT&CK 獲得威脅情報(如對特定攻擊組織所使用之技術分析等)，規劃威脅獲取與回應計畫。

4. 結論

本報告透過美國與台灣發生之勒索病毒攻擊事件，分析駭客鎖定高度電腦科技化，卻缺乏相對應資安基礎設施的區域型城市展開攻擊。藉由 BGP 遭劫持之資安事件，突顯網路基礎設施的脆弱與日常維運管理的重要性。國內部分，分析政府資安威脅現況，發現事件原因以「非法入侵」類型為主，其次為「網頁攻擊」。針對本季全球與政府所面臨的主要資安威脅，本報告就「委外管理」、「勒索軟體防範」及「BGP 組態安全管理」方面，提出資安防護建議。

資安專題分享探討 4G 運作網路漏洞與 5G 網路之安全規劃重點。隨著下一代行動通訊技術 5G 的研究脈絡，在提升行動網路用戶服務體驗的基礎上發展新服務、新架構及新技術，同時亦會對資安或用戶隱私保護衍生出新的挑戰。由於目前正值 5G 相關技術與規範發展之萌芽階段，此過渡期 4G 與 5G 網路將並存實現，因此研析 5G 系統網路所面臨的資安問題與需求時，亦應兼顧研析原有 4G 核心網路漏洞之解決方案，並持續觀測 5G 技術之安全提升

本季資安技術研析探討主題為「基於網頁漏洞之攻擊技術研析」，深入探討攻擊者行為資料庫所帶來之優勢與共通語言。ATT&CK 知識庫可被運用在開發政府、企業及網路各項安全產品與服務中之特定威脅模型與方法的基礎。ATT&CK 針對攻擊流程的定義，提出更具系統性的歸納，藉由建立簡單易懂的模型與通用語言，可以讓各家資安業者在說明網路攻擊方法時，有統一的標準去依循。對於政府機關與企業則可以透過這樣的工具，更方便地理解攻擊者行為帶來的安全風險。

下一季「資通安全技術報告」，除持續分析全球與國內政府機關之資安威脅現況，以及蒐集新興資安議題，從國內外情資與相關研究人員角度提供防護重點。有鑑於傳統密碼安全性不足的疑慮不斷，帳號遭盜用的資安事

件層出不窮，且後續事件衍生的憑證填充攻擊對組織或個人的影響更是雪上加霜。因此，下一季資安專題將探討無密碼時代之網路身分認證標準議題，提供未來身分認證另一項安全選擇。

資安相關活動

本季行政院資通安全處辦理多項資安相關活動，活動細節說明如下：

◆ 政府機關資安治理成熟度評審說明會

為協助資通安全責任等級列為 A、B 級機關了解資安治理成熟度評審架構與管理重點，並進行資安治理成熟度自評作業輔導，於 6 月 11 到 13 日辦理台北、台中、高雄共 4 場次政府機關資安治理成熟度評審說明會。

議程主題在說明資安治理成熟度架構，A、B 級機關如何透過資安治理成熟度評審機制相關資安治理成熟度與流程構面能力度之面向設計，經由策略面、管理面及技術面等不同問項，評鑑機關流程構面之資安能力度，進而全面了解內部之資安治理成熟度。

辦理說明會的同時，亦示範資安治理成熟度評審系統操作，機關登入系統後，藉由線上填寫各項安全事項之辦理情形，自動評鑑資安治理成熟度，了解不同面向是否已達到預定之目標值，並可分析待改善之領域。

◆ 政府資通安全防護巡迴研討會議

年度定期辦理之政府資通安全防護巡迴研討會，主要為宣導最新資安防護重點與訊息，協助各機關之資通安全人員提升資通安全管理與技術認知。108 年第 1 次政府資通安全防護巡迴研討會，分別於台北、台中、高雄及台東等辦理共 6 場次之研習。

固定主題為資安威脅趨勢與案例分享，期透過國內外發生之資安事件與相關趨勢，提醒機關人員注意相關之弱點或攻擊手法，並提供防護建議與作為，以利機關即早準備與回應相關威脅。另外，因應「資通安全管理法」施行，說明資安情資分享規範與進行期中檢討與精進建議。

最後一個主題為政府資訊作業委外安全，諸多政府資訊作業委託廠商建置

與維護，但相關監督與管理應持續辦理，透過委外安全主題之研討，分析相關風險與各機關應辦理之委外資安管理事項。