108年第4季資通安全技術報告

Quarterly Technical Report

目　次

圖 目 次

摘要

「第 4 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，並提供相對應之資安防護建議。同時，藉由資安專題之分享與資安技術之研析，提供政府機關於資安風險的關注重點。

「第 4 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 起案例為科技大廠發生員工竊取客服資料庫內容；另一起案例探討駭客鎖定全球運動與反禁藥組織展開攻擊。

分析政府資安威脅現況，發現政府機關通報事件原因以系統遭入侵(占 18.64%)為主，其次分別為網站設計不當(占 10.18%)與設備毀損(占 10.18 %)。

●2.資安專題分享

資安專題分享主題為基於開放標準 OpenFlow 之 SDN 資安分析。在 SDN 的技術發展上，以開放網路基金會(ONF)所致力推動之 OpenFlow 開放標準最為業界採納與遵循。專題概述基於 OpenFlow 之 SDN 資安威脅，分別從資料層、控制層及應用層列舉代表性攻擊，並就相關解決方案進行說明。

●3.資安技術研析

資安技術研析主題為探討如何部署 DNS 沉洞(Sinkhole)機制，並進行網路連線情蒐分析。行政院國家資通安全會報技術服務中心(以下簡稱技服中心)長期透過惡意電郵威脅情蒐機制，挖掘惡意程式與連線中繼站，提供惡意中繼站黑名單，協助政府機關進行資安聯防。

●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。資安專題分享基於開放標準 OpenFlow 之 SDN 資安分析，概述資料層、控制層及應用層等代表性攻擊，並就相關解決方案進行說明。此外，透過資安技術研析，探討如何部署 DNS 沉洞(Sinkhole)機制，並進行網路連線情蒐分析。

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。第 4 季(以下簡稱本季)探討組織在面對外部資安威脅戒慎以對外，更應正視內部可能之資安風險，如內部員工或委外供應鏈等。同時面對與不同一般傳統式攻擊，組織在面對進階持續威脅(Advanced Persistent Threat, APT)更應擬定多層次縱深防禦方案。

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

資通安全最大的威脅是來自於人員，但往往被關注的對象為外部駭客。在資安事件案例中，可以發現人員威脅還包含來自於內部員工。內部員工對資安所造成的威脅又可分為無心或惡意者，員工未經適切之資安教育訓練或資安規範約束，操作失誤可造成嚴重影響；而惡意之員工，在利用本身權限或任意擴張權限而造成之威脅，除在第一時間無法即時發現外，所造成之傷害更甚於外部駭客。同時，駭客因其特定目的，鎖定相關組織進行攻擊，因長時間鎖定目標，也讓受駭組織不堪其擾，進而逐步提升防護之費用。

本季具指標性案例，將研析科技大廠發生員工竊取客服資料庫內容；另一起案例為駭客鎖定全球運動與反禁藥組織展開攻擊。

首先，探討案例為科技大廠發生員工竊取客服資料庫內容事件。企業面臨更加險峻的內部威脅(Insider Threat)，108 年 11 月 5 日某科技大廠於官方部落格坦承，發現員工竊取客服資料庫內容，販賣給不知名犯罪組織牟利，影響近 12 萬名用戶。此次事件引起內部注意的原因，係該公司於 108 年 8 月發現不少使用該公司家用安全解決方案的用戶，接到冒名該公司客

服人員的詐騙電話，推測應有內部人員配合。至 10 月底，該公司終於確定整起事件主因，一名員工屢次大量存取客服資料庫，資料庫內含客服工單編號、用戶姓名、電子郵件信箱及部分客戶電話號碼等。這名員工將竊得資料賣給外部犯罪組織，而犯罪組織得手相關資料後，便用來撥打詐騙電話。

該公司更精確計算受害人數約為 68,000 人。由目前該公司所掌握的證據顯示，外洩資料並未牽涉到信用卡等交易資料，亦不影響企業與政府機關用戶，至於外洩資料流向，則尚未找到購買資料之犯罪組織。該公司已採取因應措施，包含立即終止未經許可帳號存取行為，並解雇該名員工，同時配合執法單位持續調查中。

第 2 起案例為駭客鎖定全球 16 個運動與反禁藥組織展開攻擊。108 年 10 月 28 日微軟威脅情報中心(Threat Intelligence Center)於官方部落格揭露，2020 年東京奧運前夕，偵測到來自 APT28 駭客集團新一波網路攻擊行動，駭客鎖定全球 16 個運動與反禁藥組織展開攻擊，但只有少數組織被成功入侵。APT28 又被稱為 Fancy Bear 或 Strontium，多家資安業者相信它是由俄羅斯軍事情報機構格魯烏(GRU)所主導的駭客集團，主要攻擊對象為各國政府、軍事及資安組織，受害者遍布全球，從德國議會、法國電視台 TV5Monde、美國白宮、北約組織到介入法國總統大選等。

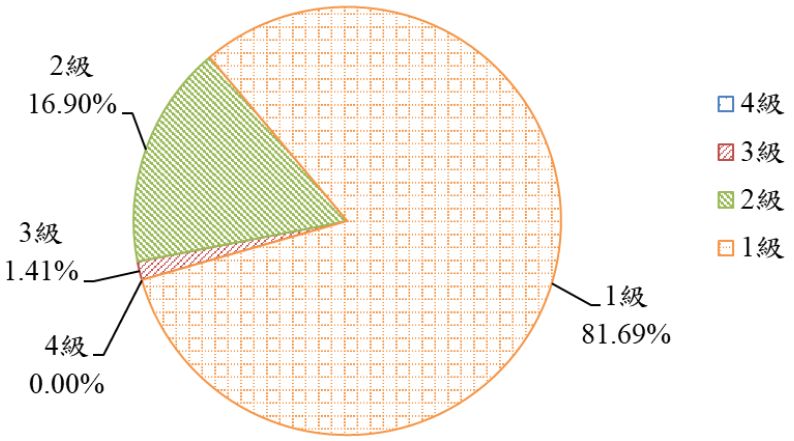
APT28 於 105 年也曾攻擊世界反禁藥組織(World Anti-Doping Agency, WADA)，據說是為報復 WADA 踢爆俄羅斯政府指導該國運動員使用禁藥一事，WADA 還要求國際奧委會(International Olympic Committee, IOC)對俄羅斯選手做出全面禁賽處分。當時 APT28 竊取 WADA 資料庫中之機密資訊，並公布奧運選手之個人機密資料。

綜覽本季重大資安事件，組織信任的夥伴包括員工或委外廠商，在擁有相關權限或資源，若不加以適當之監督或管理，所造成之資安威脅更加劇

烈。另一方面，若內部擁有機敏資料，如個人資料或財務資訊等，都會是駭客鎖定目標，則在資安防護上更應思考如何提升保護層級與縱深防禦之必要性。

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 81.69%為大宗，2 級事件占 16.9%次之，3 級事件僅占 1.41%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。



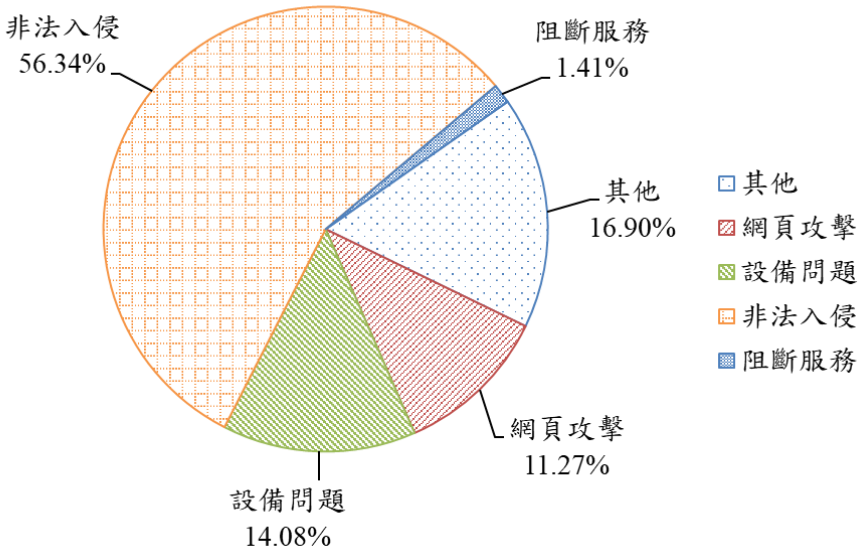
資料來源：本報告整理

圖1　108 年第 4 季資安事件影響等級比率圖

本季接獲之 3 級重要資安事件通報，為機關資通系統磁碟陣列硬碟故障，導致系統服務中斷，影響業務服務，因該系統屬核心資通系統，故通報為 3 級事件。該系統經搶修後，於可容忍中斷時間內回復正常運作，評估衝

擊與影響範圍不大。雖然政府機關仍通報零星勒索病毒攻擊事件，但因未成功入侵重要系統與資料，且因備援與備份政策在機關推廣已見成效，因此所造成之業務影響有限。

此外，資安事件通報類型依其所發現之異常情形，包含非法入侵、網頁攻擊、設備問題、阻斷服務及其他。其中，以「非法入侵」(占 56.34%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」事件分別為主要通報事件類型，詳見圖 2。



資料來源：本報告整理

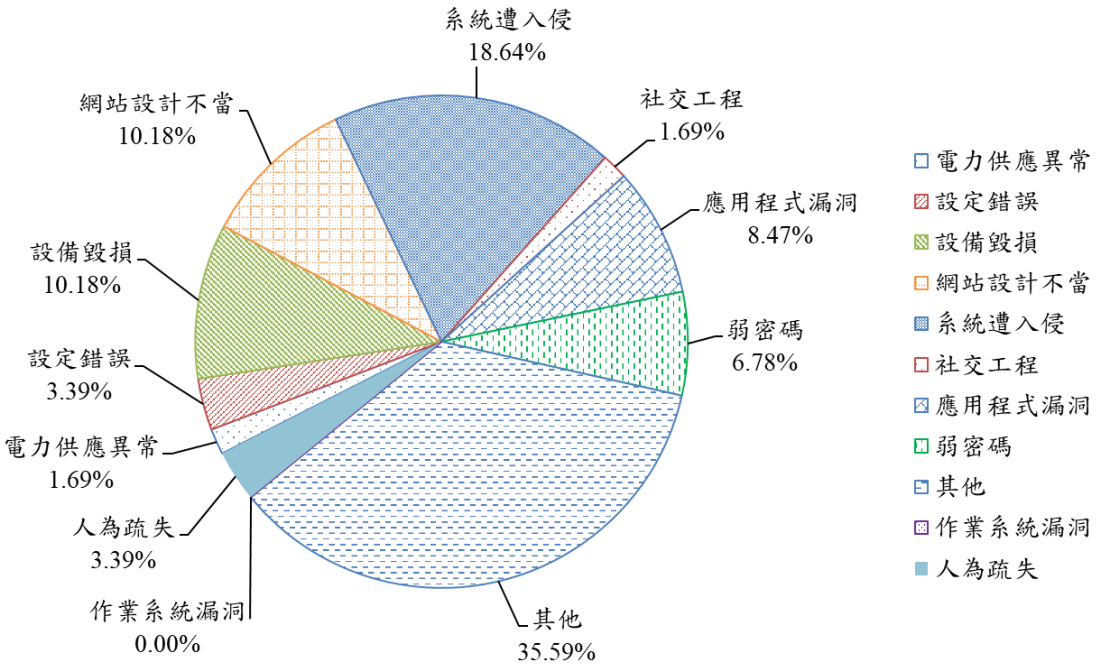
圖2　108 年第 4 季資安事件通報類型比率圖

最後，分析通報事件發生原因，以其他(35.59%)與系統遭入侵(18.64%)為主，其次分別為網站設計不當(10.18%)、設備毀損(10.18 %)、應用程式漏洞(8.47%)、弱密碼(6.78%)、人為疏失(3.39 %)、設定錯誤(3.39%)、社交工程(1.69%)及電力供應異常(1.69%)，詳見圖 3。本季事件之「系統遭入侵」占比高居第 2 位，可見雖然政府機關持續加強資安防護，但防禦上仍有待改善空間。因此，機關應不間斷辨識與檢測內部防護之弱點，加強資安防

禦等級。

分析第 4 季資安事件，網站設計不當與應用程式漏洞約占事件 2 成，顯見不論是系統開發或應用程式之資安弱點，都讓駭客有機可乘。除系統開發未遵循安全系統發展生命週期、未定期更新程式，在這些通報之資安事件中，亦發現有第三方套件漏洞遭利用，進而被植入惡意程式之情況發生。

另一項待觀察事件發生原因為設備毀損，其占比在前三名之列。雖然多數政府機關已建置備援機制，因此單一設備毀損尚能在可容許中斷時內回復，惟設備之定期維護仍為必要工作事項。



資料來源：本報告整理

圖3　108 年第 4 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，對於科技大廠發生員工竊取客服資料庫內容，除提醒機關在著重於防範外部駭客時，對於內部員工或是委外廠商亦

應訂定相關管理規範與監督資安落實情形，確保資安防護之完備性。在進階持續性滲透攻擊風行的情況下，除強化傳統資安，就現有防護工具進行全面補強，更應考量多層次或是縱深防禦等措施。

分析政府機關通報的資安事件可看出，系統開發或是應用程式的漏洞，包含程式漏洞或第三方套件的問題所造成之資安事件比例偏高，雖然長期以來宣導應用程式開發應遵循之安全系統發展原則，惟若要全面普及實作之資安應用，仍需規劃中長期之推廣策略。另外，資通設備安全管理雖屬老生長談議題，但也因為是日常維運作業且部分機關因有建置資通設備之備援機制，有時會造成資安管理人員掉以輕心，忽視資通設備資安防護之完備性。

綜整以上資安威脅現況，提供資安防護建議如下：

●人員資安管理

– 定期實施教育訓練並評估其成效，包含資安規範與專業技能之要求。

– 以最小權限開放存取，並定期檢視人員之存取權限與活動日誌。

– 定期檢視閒置帳號或預設帳號留存之必要性，避免誤用之可能性。

●第三方套件資安管理

– 盤點內部資通系統所使用之第三方套件，並造冊管理。

– 檢視使用第三方套件之組態設定，訂定資安基準防護措施。

– 關注第三方套件官網公告之更新程式，並立即更新。

●設備資安管理

– 定期盤點與更新相關設備清冊，並依資通設備機敏等級訂定設備資安管理程序。

– 定期辦理資通設備之風險辨識與分析，評估風險等級之適切性。

– 定期檢視資通設備之容量與可用性基準，並留存相關維護紀錄。

2. 資安專題分享_基於開放標準 OpenFlow 之 SDN 資安分析

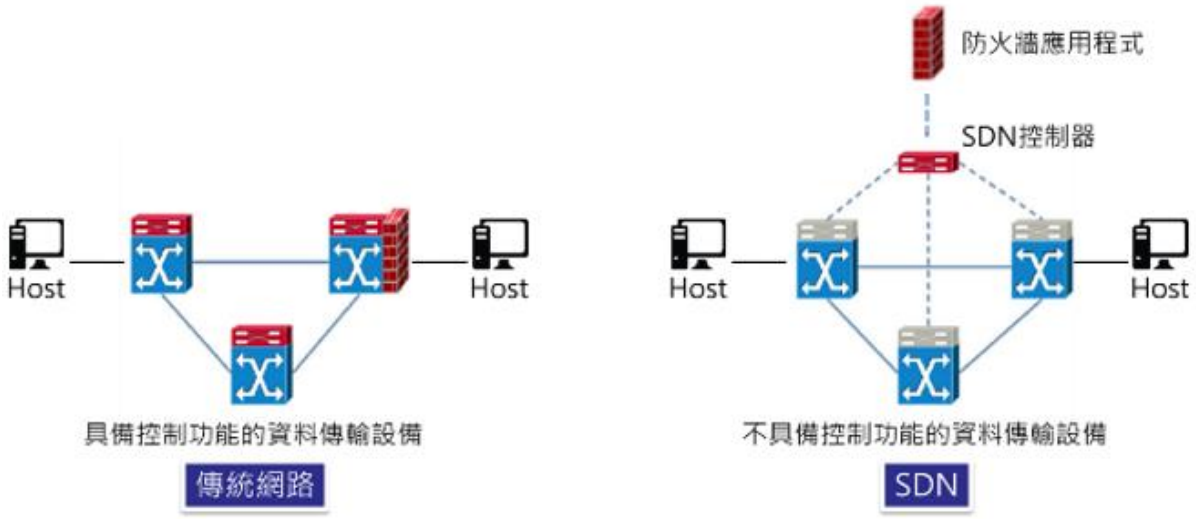
軟體定義網路(Software Defined Networking, SDN)之發展動機，在於解決傳統網路長期以來面臨的相關問題，包含建置大型網路時，網路管理與組態設定耗時且複雜、網路設備的部署利用缺乏彈性、硬體成本高及網路設備過多的控制運算與廣播傳輸使得效率不彰等議題。

SDN 與網路功能虛擬化(Network Functions Virtualization, NFV)是雲端運算、5G 網路及物聯網等新興網路核心技術。在 SDN 技術發展上，又以開放網路基金會(ONF)所致力推動的 OpenFlow 開放標準，最為業界採納與遵循。在行政院核定之「台灣 5G 行動計畫」與「建構公教體系綠能雲端資料中心計畫」中，SDN/NFV 即扮演網路建構之核心技術。

然而，SDN/NFV 新形態的網路運作概念與整合應用的創新發展，也必然會同時帶來新的資安威脅與挑戰。因此，本報告基於 OpenFlow 開放標準，對 SDN 之架構與資安威脅進行研析。

2.1 SDN 架構說明

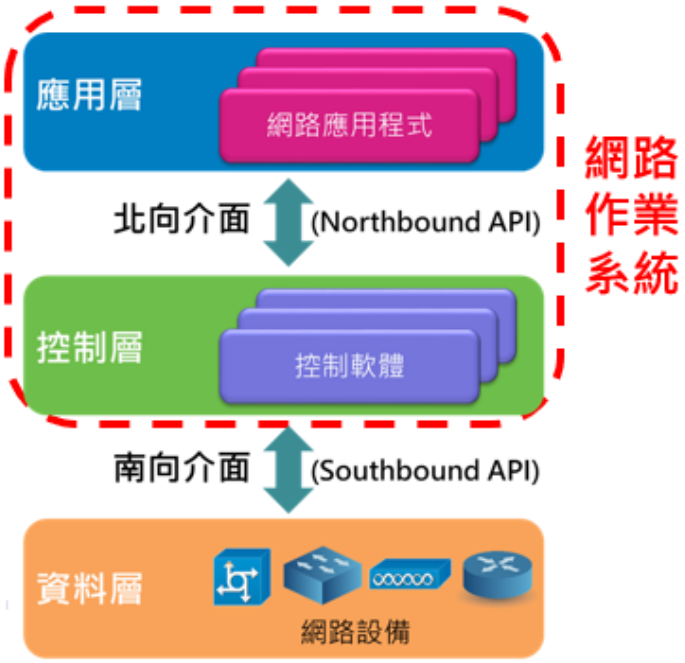
傳統網路與 SDN 網路的差異在於，SDN 將傳統網路設備的控制功能抽離出來(控制層)，讓網路設備只剩下單純的資料傳輸(資料層)，由控制層的控制軟體集中控管網路，提升網路資源的使用彈性與效率，詳見圖 4。



資料來源：本報告整理

圖4　傳統網路與 SDN 網路的差異

SDN 之架構分為資料層、控制層及應用層共 3 層，詳見圖 5。



資料來源：本報告整理

圖5　SDN 架構

資料層：負責封包的轉傳，網路設備根據封包處理表(Flow Table)中的封包處理規則(Flow Rule)來處理進入的封包，若不存在該封包處理規則，則需向控制層詢問並更新處理規則，資料層的網路設備統稱為交換器(Switch)。

控制層：由集中式的控制器(Controller)統一負責路由計算、拓樸管理及流量監控，是 SDN 的核心。向上透過北向介面與應用層溝通，目前尚未有共通標準，向下透過南向介面與資料層溝通，OpenFlow 是主要的共通標準。

應用層：由應用程式執行各種網路服務，如負載平衡、防火牆及流量分析等。

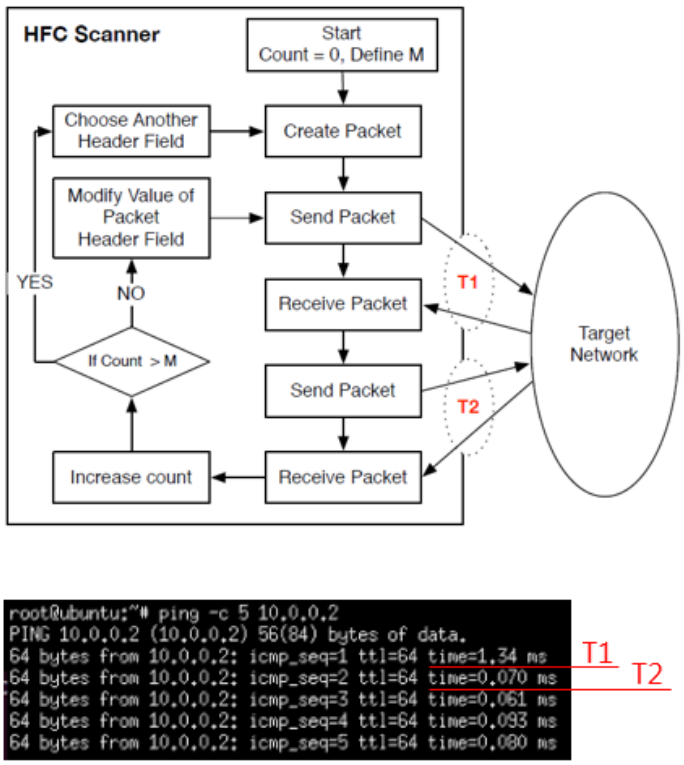
2.2 基於 OpenFlow 之 SDN 資安分析

OpenFlow 是開放網路基金會(ONF)所制訂的 SDN 開放標準，主要定義交換器功能與交換器與控制器通訊協定等 2 大部分。基於 OpenFlow 標準，參考國際相關資安標準與文獻，彙整在 SDN 資料層、控制層及應用層之代表性攻擊，分別為「封包流規則洪水」、「拓樸中毒攻擊」及「惡意應用程式」，以下將說明各層之代表性攻擊與相關解決方案。

- 封包流規則洪水

  封包流規則洪水為藉由大量向控制層詢問與無意義的處理規則，導致阻斷服務(Denial of Service, DoS)攻擊。攻擊流程開始將先探測攻擊目標是否為 SDN 網路，並連續傳送兩次相同封包，假設第一個封包(封包 1)會詢問控制器，那麼更新處理規則後第二個封包(封包 2)將不再詢問，因此封包 1 的處理時間(T1)會大於封包 2 的處理時間(T2)。透過 T1 與 T2 的多次統計測試，即可確認是否為 SDN 網路。接續探測處理規則所判斷的封包欄位，選擇封包欄位並多次改變該欄位值，符合 T1

大於 T2 欄位即為處理規則的判斷欄位，依封包判斷欄位產生並傳送大量封包。假設判斷欄位包含目的地 IP 位址，攻擊者可在 30 秒(處理規則的存活時間)內傳送 1,500(flow table 容量)個不同目的地 IP 位址封包，以造成後續正常封包傳送嚴重延遲(詳見圖 6)。



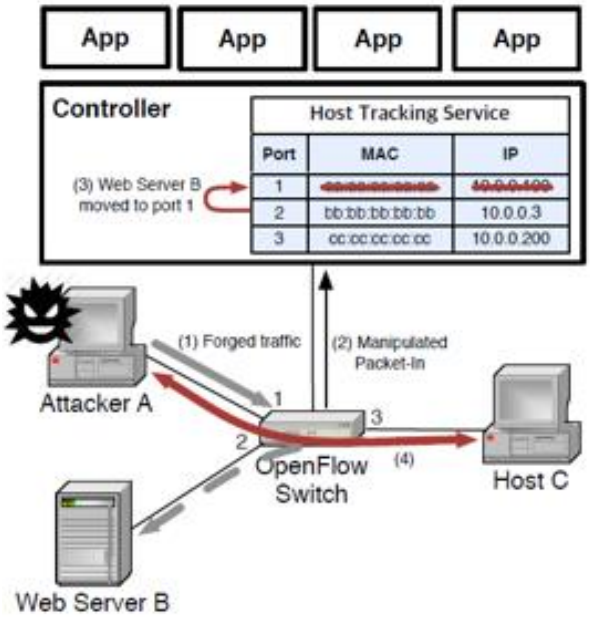
資料來源：本報告整理

圖6　封包流規則洪水攻擊流程

面對封包流規則洪水之解決方案，可針對網路連線白名單建立交換器靜態處理規則，以確保大部分日常通訊正常傳輸，並在控制器建立封包處理表滿載(TABLE_FULL)偵測機制，如當 TABLE_FULL 錯誤訊息在一定時間內達到設定門檻值時，即針對該交換器特定 port，下達暫時關閉命令，並可同時縮短處理規則存活時間，以減緩交換器與控制器之間通訊壅塞，並降低控制器處理資源消耗，亦可加快清除無意義處理規則。

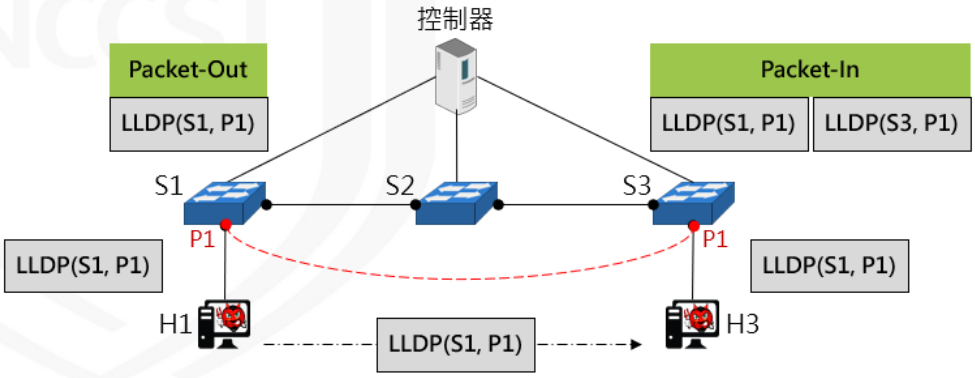
- 拓樸中毒攻擊

拓樸中毒攻擊為攻擊者利用控制器拓樸管理弱點來改變網路拓樸，進而衍生主機冒充、DoS 及中間人等攻擊。SDN 控制器利用拓樸管理來維護網路拓樸資訊，除提供整個網路可視性外，更是 SDN 網路管理與應用基礎(路由、移動追蹤及網路優化等)，駭客利用改變網路拓樸與後續攻擊，可造成二大資安威脅，第一為「主機位置劫持 (Host Location Hijacking)」，攻擊者可成功冒充目標主機，以劫持送往目標主機的網路資料，詳見圖 7；第二為「鏈結偽造(Link Fabrication)」，攻擊者利用相關服務之弱點偽造交換器間鏈結，並產生 DoS 攻擊與中間人攻擊，詳見圖 8。



資料來源：本報告整理

圖7　主機位置劫持



資料來源：本報告整理

圖8　鏈結偽造

面對主機位置劫持，解決方案可藉由驗證主機移動的正確性，採取移動前通知控制器主機將從該 port 卸載，而移動後控制器檢查原主機是否還在該 port 上，以有效驗證主機位置。

而可有效解決鏈結偽造方式，則為驗證鏈結流量的 port。以維護每個 port 的連接裝置型態，分為 HOST、SWITCH 及 CONTROLLER，然後驗證每一條鏈結流量途經的 port 不能是 HOST。

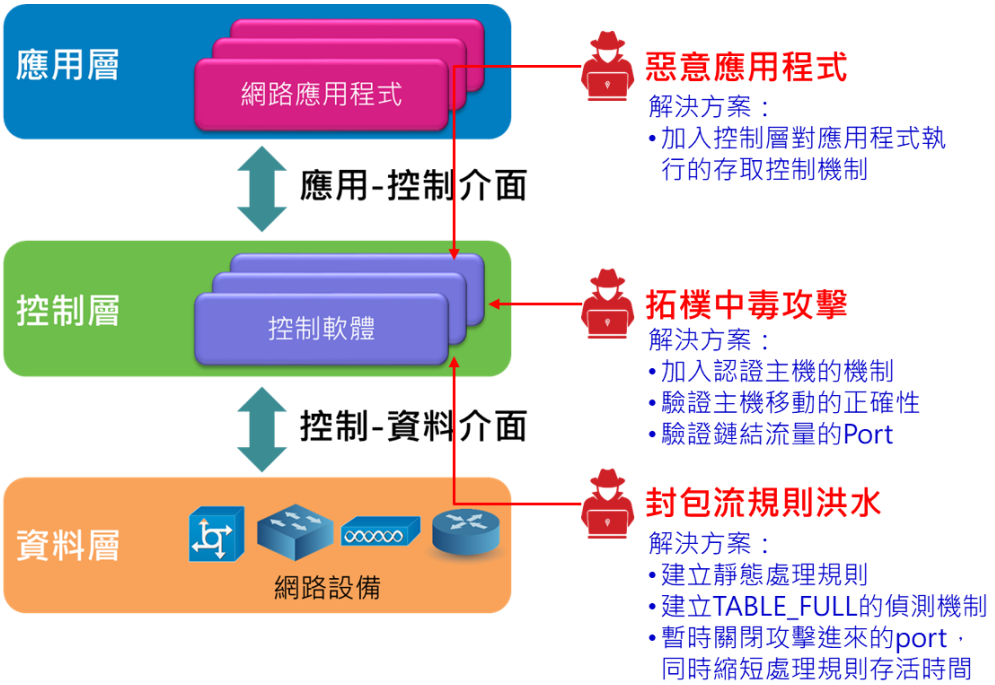
- 惡意應用程式

由於 SDN 控制層是網路作業系統核心(Kernel)，但對應用層程式缺乏存取控制資安機制，導致惡意應用程式不斷要求資源導致資源耗竭，或執行特權指令直接控制網路運作。攻擊手法為於程式中建立鏈結串列(linked list)且不斷新增節點，導致執行該應用程式的控制器程序因記憶體耗盡而中斷；或是藉由執行系統指令，於程式中呼叫 exit()函式，導致執行該應用程式的控制器程序被終止。

解決方案為設定安全的存取控制機制，SDN 控制層與應用層關係相當於作業系統中核心與應用程式關係，因此控制層對於應用層程式執行，必須有資源管理器(Resource manager)與系統呼叫檢查器(System

call checker)等安全存取機制，以有效控制程式執行。

綜整以上攻擊手法與解決方案，詳見**錯誤! 找不到參照來源。**。



資料來源：本報告整理

圖9　SDN 架構風險與因應方案

SDN 是新興網路技術，未來仍將窺見有新的相關資安議題與應用出現。因此，持續研究 SDN 相關資安攻擊與防護方案，並透過 SDN 資安驗證平台進行實證仍是重要工作。此外，為因應政府機關未來 SDN 建置規範、資安檢測及防護機制之需求，後續將規劃發展 SDN/NFV 網路規劃參考指引與建立 SDN/NFV 資安檢測能量，並探討利用 SDN/NFV 特性，加強政府資安防護之應用，如隨時監控可疑流量、建立智慧分流蜜罐系統及抗 DDoS 之頻寬調節等，以厚實政府資安防護能量。

3. 資安技術研析_DNS 沉洞(Sinkhole)機制

本季所探討的資安技術研析，是探討如何部署與利用網域名稱系統(Domain Name System, DNS)沉洞(Sinkhole)機制，進行網路連線情蒐分析。技服中心長期透過惡意電郵威脅情蒐機制，挖掘惡意程式與連線中繼站，提供惡意中繼站黑名單，協助政府機關進行資安聯防。

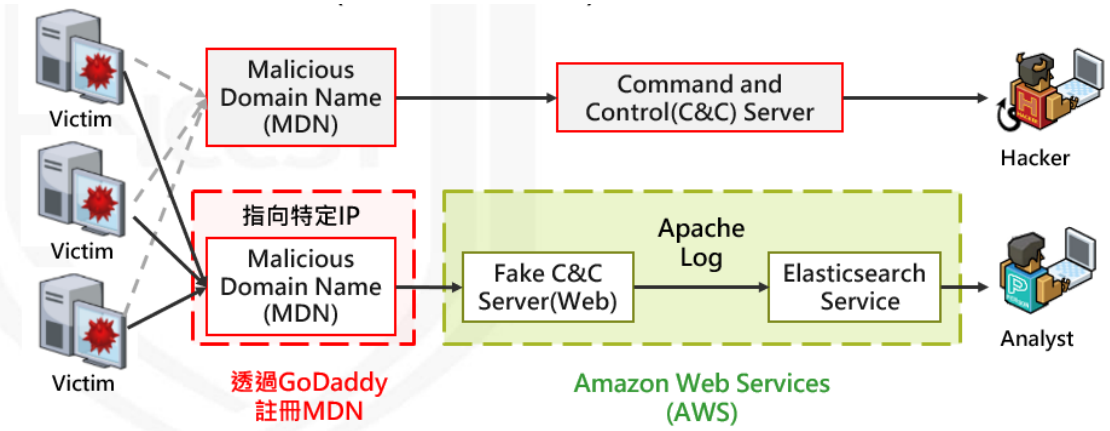
為更加精準掌握不在政府網際服務網(GSN)監控範圍內的全球受害單位，不定期清查惡意中繼站黑名單，並註冊已過期之中繼站域名，透過部署 DNS 沉洞機制，針對網路連線進行情蒐分析。

以下將說明 DNS 沉洞機制與網路連線情蒐分析成果。

3.1 DNS 沉洞機制部署簡介

DNS 沉洞機制可針對特定之網域名稱，以錯誤的結果進行回應，避免存取不必要之網路通訊，如殭屍網路或存在惡意程式網站。因此部署 DNS 沉洞機制可以是具建設性運用，如用來解析 APT 受害連線資訊、惡意中繼站及掃描探測連線資訊等威脅分析。同理，若此機制被惡意利用時，則可利用 DNS 沉洞提供錯誤資訊，讓攻擊者將系統重新導向至惡意網站。以下將概述如何架設部署 DNS 沉洞機制，並進行中繼站分析之做法。

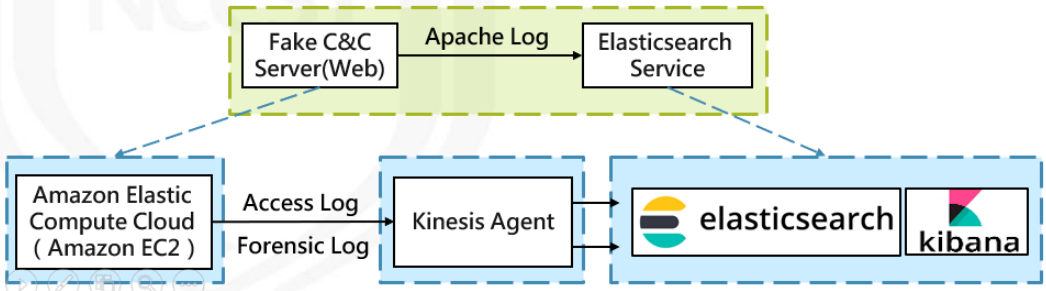
首先，使用 Amazon Web Services(AWS)架設與部署 DNS 沉洞機制，以取得受害電腦連線至 C&C 伺服器的報到資訊，網頁日誌收容利用 Apache 伺服器與 mod_log_forensic 模組，同時運用 ELK Stack 機制，進行日誌索引記錄，詳見圖 10。



資料來源：本報告整理

圖10 DNS 沉洞機制部署架構

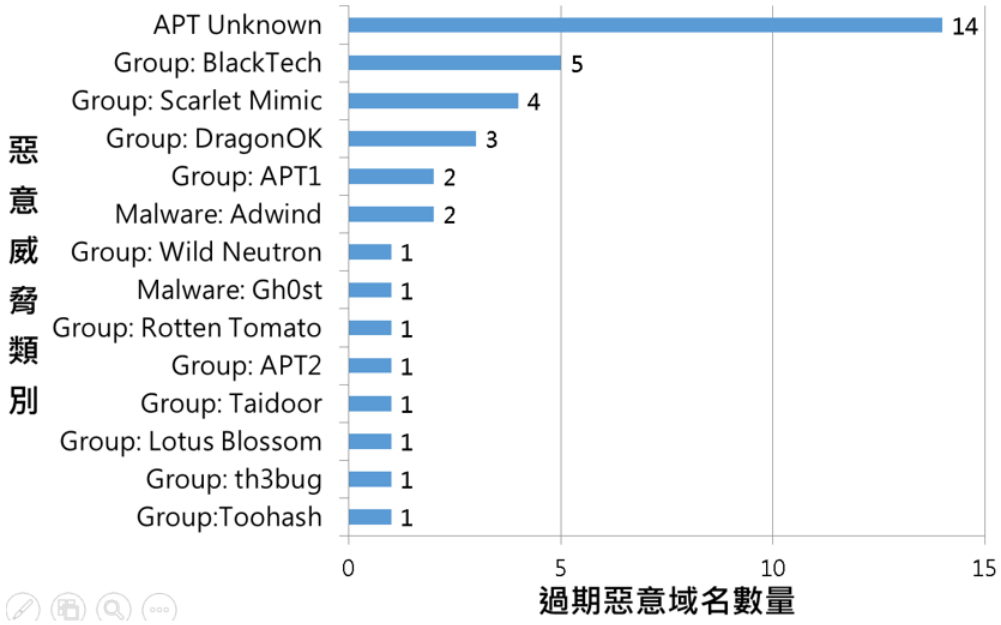
AWS 日誌收容索引架構主要包含 Elastic Compute Cloud(EC2)、Kinesis 及 Elasticsearch Service 等 3 大元件，詳見圖 11。EC2 提供 Web 服務方式，讓使用者可彈性地在雲端電腦運行虛擬機；Kinesis 將日誌等資料串流擷取、轉換及載入 AWS 資料存放區；而在 Elasticsearch Service 中，Elasticsearch 主要為分散式搜尋引擎，也是 NoSQL 資料庫的一種，Kibana 則可透過視覺與圖形化表示方式，來顯示與分析各種日誌。



資料來源：本報告整理

圖11 AWS 日誌收容索引架構

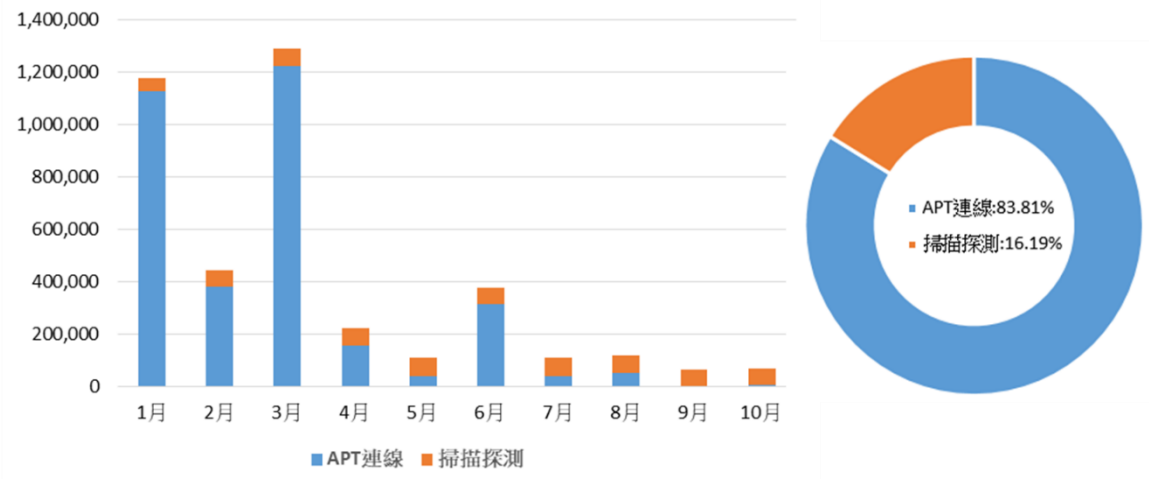
此次 DNS 沉洞機制之情蒐目標，係針對 99 年至 105 年間曾被偵測記錄的 38 個惡意中繼站域名，其列表與分類詳見圖 12。



資料來源：本報告整理

圖12 監控的惡意中繼站列表與分類

統計 108 年 1 月到 10 月之期間，共蒐集到 3,966,008 筆連線紀錄，計有 41,291 組不重複 IP 位址進行連線，其中 APT 類型之連線占 83.81%，掃描探測類型之連線占 16.19%，每月之攻擊類型統計圖詳見圖 13。



資料來源：本報告整理

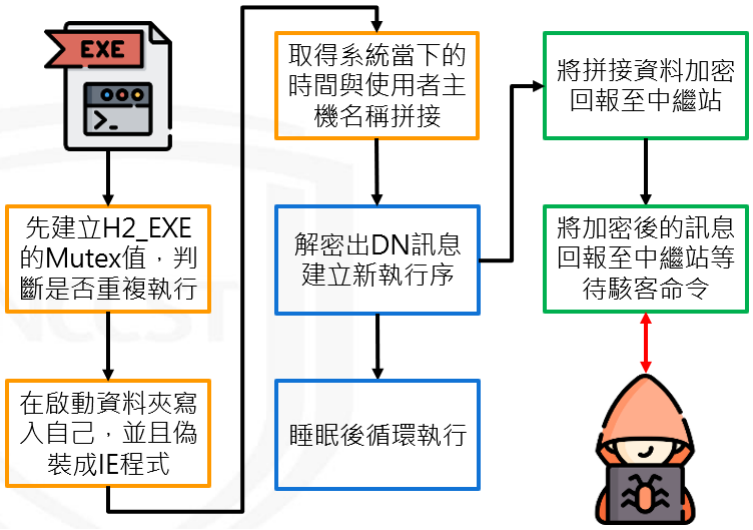
圖13 攻擊趨勢類型統計圖

進一步分析 APT 類型之連線報到紀錄，發現有 99.99%連線是來自於名為「webmailerservices.com」之中繼站，因而針對該中繼站進行深入分析。

3.2 中繼站分析

技服中心進一步針對 webmailerservices.com 進行解析，以了解有關該中繼站之相關攻擊手法。

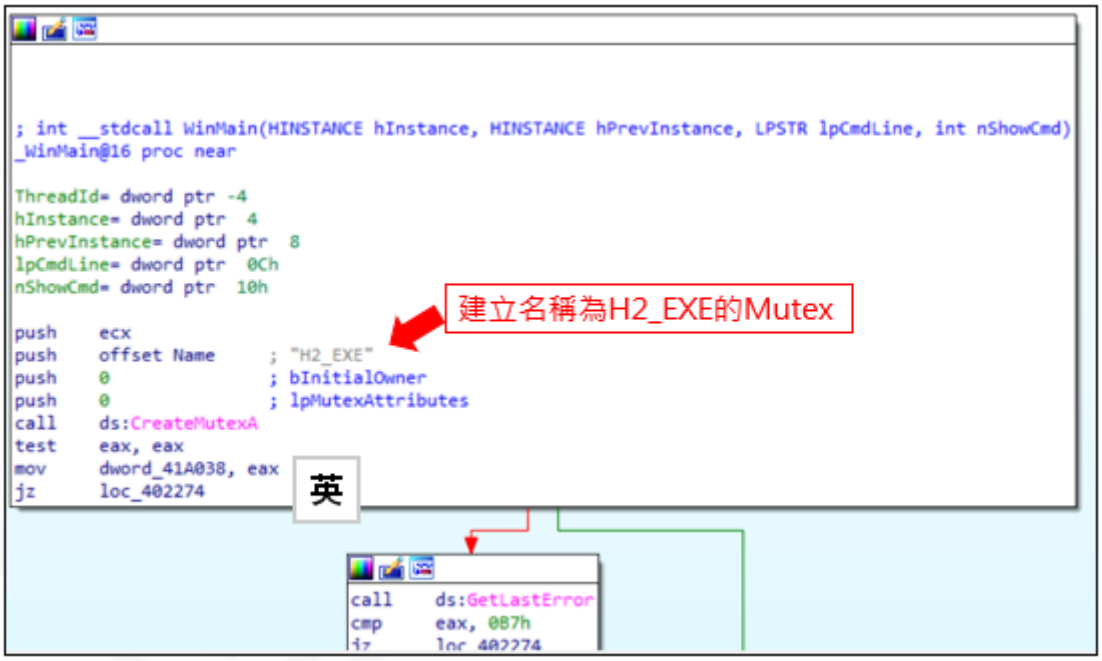
此攻擊是透過社交工程信件夾帶惡意附加檔案(惡意樣本)，寄至政府機關準備展開攻擊，逆向分析該惡意樣本之執行流程，詳見圖 14。



資料來源：本報告整理

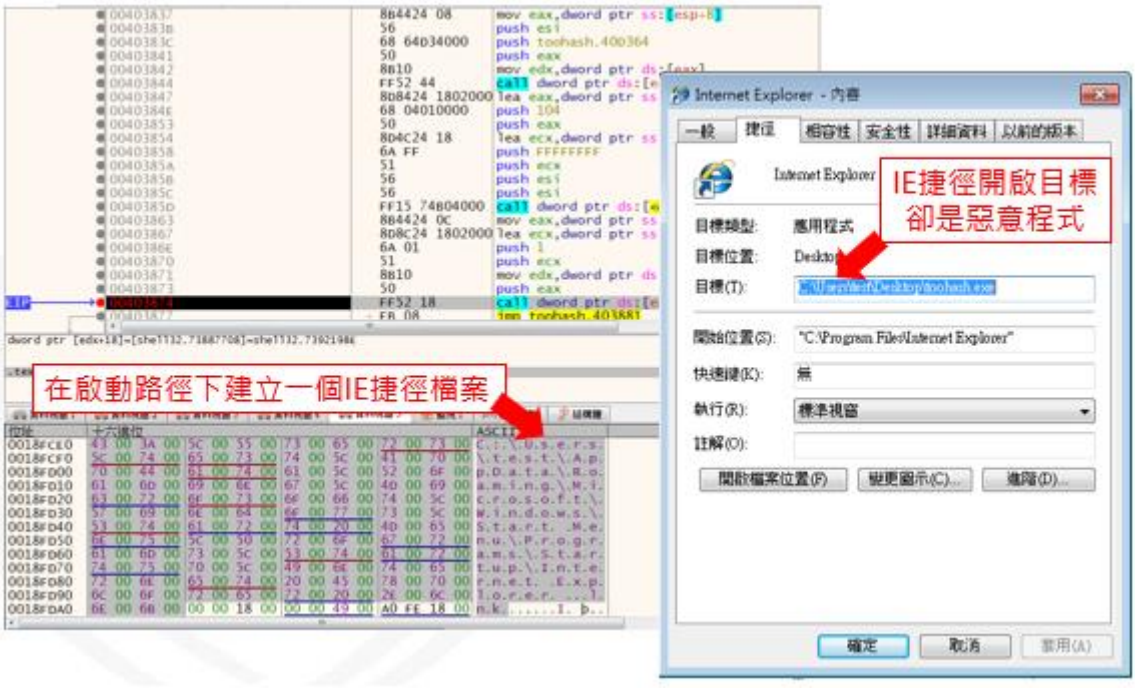
圖14 惡意樣本執行流程

首先，該惡意樣本會先建立名稱為 H2_EXE 的 Mutex 值，再將啟動資料夾之路徑設為連線至 IE 捷徑檔，而該 IE 捷徑檔的開啟目標則為惡意程式(詳見圖 15 與圖 16)。此外，該惡意樣本還可取得主機名稱與主機時間等系統資訊，並拼接相關結果，以利後續回報至中繼站。



資料來源：本報告整理

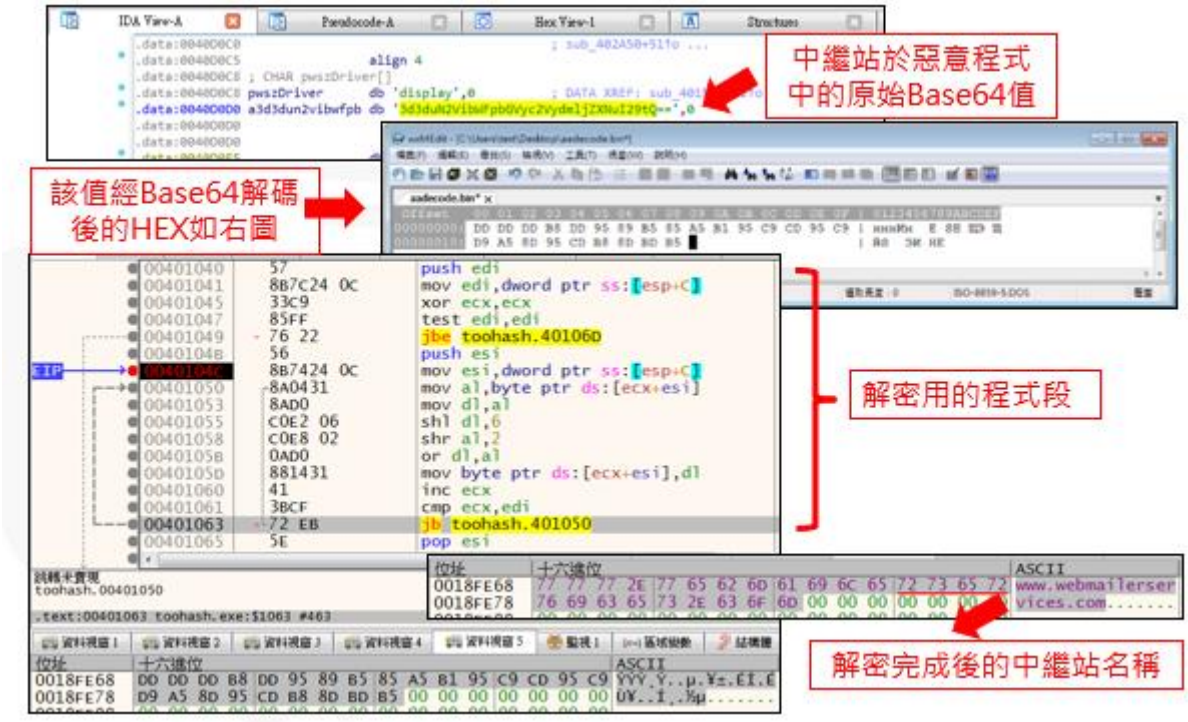
圖15 建立 Mutex 值



資料來源：本報告整理

圖16 啟動路徑建立惡意程式

藉由分析惡意樣本之程式碼內容，可將經由 Base64 編碼之中繼站名稱進行解密，並得到中繼站名稱「webmailerservices.com」，詳見圖 17。後續該惡意樣本會將先前所得知之主機系統資訊加密回報至中繼站，並完成攻擊。



資料來源：本報告整理

圖17 解密中繼站

技服中心透過此 DNS 沉洞機制，情蒐與分析 GSN 監控範圍外之受害電腦資訊，並揭露過往 APT 族群仍在進行活動。相關成果後續可進一步提供給受害目標所屬之國內電信業者，以協助清查受害之電腦資訊，或藉由「國家資安資訊分享與分析中心」(National Information Sharing and Analysis Center, N-ISAC)分享相關資安情資。此外，未來亦可針對其他惡意域名取得對特定.TW 域名之相關惡意攻擊情蒐分析。

4. 結論

本報告本季具指標性案例，透過科技大廠發生員工竊取客服資料庫內容，分析資安事件發生在內部威脅，如來自員工或夥伴時如何防患於未然，且能即時發現並處理。另一起案例為駭客鎖定全球運動與反禁藥組織展開攻擊。駭客鎖定特定目標之攻擊，通常藉由長時間入侵、滲透規劃及執行動作，包含偵查與蒐集資料等，以成功發掘目標對象之資安漏洞或弱點，因此入侵成功機率大增，這種進階持續攻擊也成為組織所面臨的最大威脅來源之一。國內部分，分析政府資安威脅現況，發現事件原因以系統遭入侵為主，其次分別為網站設計不當及設備毀損。針對本季全球與政府所面臨的主要資安威脅，本報告就「人員資安管理」、「第三方套件資安管理」及「設備資安管理方面」，提出資安防護建議。

資安專題分享基於開放標準 OpenFlow 之 SDN 資安分析，參考國際相關資安標準與文獻，彙整在 SDN 資料層、控制層及應用層之代表性攻擊，分別為「封包流規則洪水」、「拓樸中毒攻擊」及「惡意應用程式」，並就相關解決方案進行說明。

此外，透過資安技術研析，探討如何部署 DNS 沉洞(Sinkhole)機制，並進行網路連線情蒐分析。深度分析 APT 類型之連線報到紀錄，發現有 99.99%連線是來自於名為「webmailerservices.com」之中繼站，此攻擊是透過社交工程信件夾帶惡意附加檔案，寄至政府機關展開攻擊。相關成果後續可進一步提供給受害目標所屬之國內電信業者，以協助清查受害電腦資訊，未來亦可針對其他惡意域名取得對特定.TW 域名之相關惡意攻擊情蒐分析。

資安相關活動

本季行政院資通安全處(以下簡稱資安處)辦理多項資安相關活動，活動細節說明如下：

◆ 資安策略會議

資安處於 12 月辦理資安策略會議，主題著重於第六期國家資通安全發展方案之相關發展議題。對於即將進入萬物聯網、即時網路的社會，資安議題勢必面臨更加嚴峻的挑戰。因此除產業創新與數位國家 2 大政策外，資安將是重要的基礎。

基於打造資安即國安 2.0 戰略，暨「資安之國」的目標，在以資安為後盾的背景下，施行產業創新與數位政府治理願景。此次策略會議邀請資安各界專家提出對第六期國家資通安全發展方案有策略與方案之擘劃與指導，規劃不同分組，以進行深度研討。分別有「深度防禦組」、「法規標準組」、「產業自主組」及「人才培育組」。會後並蒐整分組報告簡報及委員回饋意見，做為修正第六期發展方案之參考。

◆ 跨國網路攻防演練

行政院國家資通安全會報 108 年 11 月 6 日至 8 日，辦理為期 3 天跨國網路攻防演練(Cyber Offensive and Defensive Exercise, CODE 2019)，本次演練有別於過去以情境演練方式，108 年首次改採實兵演練方式辦理，邀請國內外政府資安攻擊好手，與我方金融機構組成之防守聯隊共同進行實戰演練，提升彼此資安專業技術與應變能力。

鑒於各國金融機構常為組織型駭客所鎖定目標，特別設計以金融資安環境為主軸，由金融機構實戰好手組成資安防守聯隊，實際進行攻防對戰之演練。此次跨國網路攻防演練有幾項重要發現，包含透過適當組態設定調整與配置防火牆與網站應用程式防火牆(WAF)等防禦設備，可成功阻擋來自

於外部之攻擊行為；滲透內部執行攻擊主要是透過取得帳密或是藉由內部的跳板機，針對網頁或資料庫等系統攻擊取得所需情資；機關資通系統仍存在作業系統安全性更新未安裝等議題。