作業報導

●臺中市政府導入 APT 資訊安全防護機制簡介

臺中市政府資訊中心設備網路科高級分析師 陳凱

壹、 背景說明

一、APT 的生命週期

APT（Advanced Persistent Threat，進階持續性攻擊）是針對特定組織所作的複雜且多方位的網路攻擊。APT 攻擊重點在於低調且緩慢，利用各種複雜的工具與手法逐步掌握目標的人、事、物，並不動聲色地竊取其鎖定的資料。2013 年，美國網路安全公司麥迪安（Mandiant）發布了關於 2004 至 2013 年間疑似來源於中國的 APT 攻擊的研究結果，其攻擊生命週期如下：

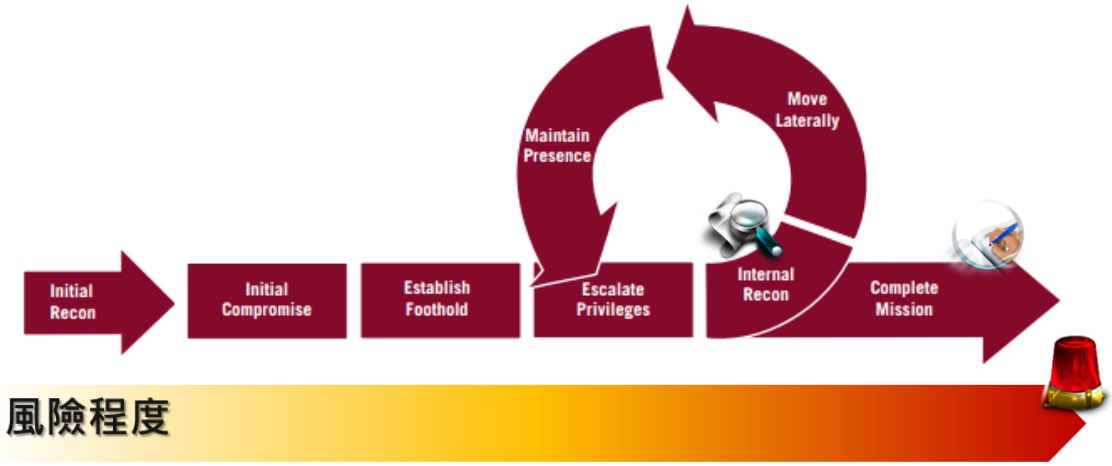

圖 1　APT 生命週期

(一) 初始入侵(Initial Reconnaissance & Compromise) － 使用社交工程、釣魚式攻擊、零時差攻擊、社交郵件等方法進行。在受害者常去的網站上植入惡意軟體（掛馬）也是一種常用的方法。

(二) 站穩腳跟(Establish Foothold) － 在受害者的網路中植入遠端連線工具（如木馬 Malware），打開網路後門，實現隱匿性連線操控(CNC, Command and Control)。

(三) 提升特權(Escalate Privileges) － 通過利用漏洞及破解密碼，獲取受害者電腦的管理員特權，並可能試圖獲取 Windows 網域(Active Directory)管理員特權。

(四) 內部勘查(Initial Recon) － 收集周遭設施、安全信任關係、網路結構的訊息。

(五) 橫向發展(Move Laterally) － 將控制權擴展到其他工作站、伺服器及設施，以收集數據。

(六) 保持現狀(Maintain Presence) － 確保繼續掌控之前獲取到的連線許可權和權限。

(七) 任務完成(Complete Mission) － 從受害者的網路中傳出竊取到的資料。

二、APT 事件頻傳

102 年 3 月，南韓多家金融機構、廣播公司等國家關鍵基礎機構遭到攻擊，導致服務癱瘓，同年 4 月，國安局副局長張光遠透露健保局全民個資遭駭外洩（未含病歷）案，同年 5 月，本國政府所用電子公文交換系統遭駭，全國各機關

皆大動作重灌公文系統及設定更嚴謹之防火牆規則，103 年 1 月，遠通電收系統在三小時內遭到八十二億次的網路駭客攻擊，行政院副院長毛治國指出，「這是非常惡意的攻擊」；政務委員張善政亦認定這是「非常嚴重」的第三級攻擊。103 年 12 月，據路透社報導，美國政府已經確認 Sony 影業被駭事件與北韓政府有關，由於駭客威脅稱將會在「名嘴出任務」（The Interview）這部電影上映時，對電影院發動恐怖襲擊，Sony 影業被迫將該影片線上上映及小規模戲院上映。部分專家預估 Sony 此次的損失約 1 億美元。

依據趨勢科技 102 年調查，科技業平均要花 11.5 個月才會發現被駭，政府單位平均要 8.5 個月才會察覺被駭。102 年美國網路安全公司 Mandiant 公布報告，直指中國(大陸)解放軍 61398 部隊，代號為「APT1」之中國(大陸)「網軍」負責向英語系國家進行網路偵蒐攻擊的解放軍長時間、定期侵入受害機構網路，廣泛竊取智慧財產、技術藍圖、製造規程、實驗結果、商業計畫、議價文件、聯盟協議及大量電子郵件，全年無休侵入受害機構和人士的電郵，最長期間達 4 年 10 個月。141 個 APT1 受害機構中，87%為英語系國家的機構總部，這些產業符合中國所宣稱，12 次 5 年計畫 7 大策略性成長產業中的 4 項。面對中國(大陸)十八萬「網軍」部隊威脅，行政院資通安全辦公室主任蕭秀琴於 104 年 1 月坦言：「台灣已成為中國駭客試驗場域、資安環境相當嚴峻。」由此可知 APT 攻擊之威脅不容再被忽視。

三、臺中市政府積極防禦 APT

本府管理大量的個人(民眾)資料及公務機密文件，這些資料必需有效被保護，面對新型態的 APT 攻擊，為避免被本府機敏資料被竊取，實需建置防禦 APT 攻擊及保護機敏資料之安全機制。為加強本府資訊服務之防護能力，本府所有電腦、系統之網路環境，都須納入安全防禦機制，以便建立一套緊急應變措施，確保本府資訊作業的安全，因此自 102 年起積極推動資料中心骨幹升級計畫，建構 APT 感知防護網，以及 APT 智慧防駭自動回饋系統。以強化智慧政府治理的內涵，並提升資訊服務、機密資料以及駭客攻擊防護等能力。

貳、 APT 資訊安全防護服務機制

資訊中心網路設備科張碧顯科長表示：「APT 的防禦，絕對不是一個產品的運用，而是一個服務及策略的規劃。一個產品的功能，或許可以滿足現階段的需求，但面對日新月異的 APT 攻擊，光靠產品的功能很快就會過時。所以，唯有精準的策略及良好的服務，才可以應付各種新型態的攻擊。」

本府於 103 年 6 月導入資訊安全防護作業委外服務案（以下簡稱本專案），防護範圍涵蓋本府 135 所機關，並保護 13,561 台用戶端(Server, PC)，並應用國內防毒大廠提出的 APT 三大應對策略，分別是提高攻擊門檻、提高感知能力、提高處理能力。這次因應 APT 攻擊所採取的強化建置，目標就放在提高感知能力。此外，除了導入 APT 防護系統及維運管理機制，監控及處理服務更是不可或缺的要件，這有助於掌握 APT 威脅資訊、研判與因應資安風險，並提供即時的安全監控及緊急處理。

一、提高攻擊門檻

除了現有的防火牆及入侵偵測等資安設備外，本專案導入骨幹網路 APT 閘道設備及郵件閘道設備，即時的在網路傳輸路徑中進行偵測威脅事件(含 Malware-CNC、Blacklist DNS、Malware-Backdoor)並加以阻擋，並針對惡意社交郵件進行偵測及攔阻，減少第一階段攻擊成功的機率，這個部分通常是各機關最難處理，也是成本最高的部分。

二、提高感知能力

本專案導入網路威脅偵測設備及端點(Server, PC)防護軟體，以過濾內網可疑的網路行為，偵測內網惡意程式活動的機制，並部屬端點防護軟體進行鑑識、追蹤、採集 LOG 及惡意程式，具雲端沙箱功能感知防毒軟體無法偵測到的惡意程式活動，工作目標在於早期發現內部被植入遠端連線工具，並全面的清理。

三、提高處理能力 － 制訂 APT 事件處理機制

本府將 APT 依據緊急程度分成 A、B、C 三類事件，A 類為「國家資通安全會報技術服務中心」通報需立即處理事件，於上班期間內接獲通報後，本專案人員須於 1 小時內到本中心報到並開始執行事件處理。B 類為本府 ISMS 及防毒專案 SOC（Security Operation Center）通報事件，本專案人員須於 1 日內執行事件處理。C 類為每月相關檢討會議交辦事件。APT 案件管理機制如下：

(一) 由事件通報起建立案件納管。

(二) 控管所有案件直到結案。

(三) 案件緊急處置建議。

(四) 定期通報案件處理階段及分析結果。

(五) 每月彙整所有案件及呈報案件進度。

(六) 提供案件處理結案報告。

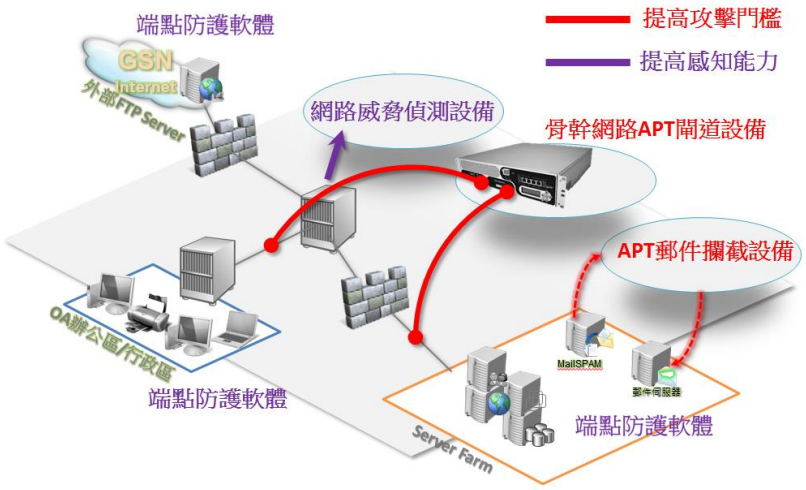

圖 2 網路防護架構

參、 APT 案例分析

本專案處理 A、B、C 三類事件時，採現場或遠端連線按 SOP 進行，首先備份受害者電腦或主機所有資料，避免資料在鑑識過程誤刪，再安裝端點防護軟體進行

鑑識、追蹤、採集 LOG 及惡意程式，經過幾天的沙箱運作及 LOG 收集後，如偵測、捕獲到未知惡意程式活動時，除進行隔離或清除動作外，必要時後送防毒軟體實驗室分析並製作成病毒碼，派送至各端點防毒軟體，達到全面防護的目的（全球安裝該防毒軟體之電腦或主機亦同樣受益）。

一、案例一：本府某局處個人電腦

各級機關基本上對於被通報連線 C&C 時，一般會先以防毒軟體掃毒，如無法發現新種惡意程式，其次則整機重灌，本案例在於分享運用工具及機制找出隱藏的連線程式，並製作出相對應的病毒碼，以達全面清理之目的。

本府防毒專案 SOC 偵測到該電腦對外部已知 C&C 進行 DNS 連線行為，本專案人員至現場安裝端點軟體並發現查詢紀錄，為 11 月 16 日系統執行 rundll32.exe 時所觸發且連線 C&C(95.＊.＊.240)，並查詢 11 月 17 日所蒐集的 LOG 發現執行 rundll32.exe 時夾帶執行未知惡意程式 wstpagern.dll 及其隱藏位置，後送防毒軟體實驗室分析並製作成病毒碼。

圖 3 發現 rundll32.exe 行為異常

圖 4、發現 wstpagern.dll 惡意程式

二、案例二：從發現、阻擋木馬到根絕木馬

Chickenkiller.com 是一個已知的釣魚網域，經常被用來作為社交工程的跳板，本案例在解析閘道設備感知到不正常連線到 Chickenkiller 後，如何交互應用不同業者的工具分析找出存在主機中的惡意程式，並將特徵碼製造納入防毒體系，以達到全面防堵的目的。

本專案 103 年 11 月分析威脅事件發現未阻擋威脅事件（BLACKLIST DNS request for known malware domain chickenkiller.com，以下簡稱 Chickenkiller 事件），從封包的內容可得知 Client 進行嘗試用 DNS 去查詢可疑網址 (facsbook.chickenkiller.com)，並確認為惡意攻擊行為後即進行阻擋連線，103 年 12 月發現 chickenkiller 事件阻擋數量有 49,958 筆，104 年 1 月有 44,512 筆，當

104 年 1 月 20 日在進行本府某局處主機 APT 事件處理發現某隻惡意程式(nwagent.dll)嘗試連結相同可疑網址(facsbook.chickenkiller.com)，而當 nwagent.dll 被送防毒軟體實驗室分析並製作成病毒碼，並派送至本府各端點防毒軟體後，104 年 2 月發現 Chickenkiller 事件阻擋數量已下降至 24 筆，達到全面防堵的目的，並展現本專案從發現、阻擋木馬到全面布設防堵的整體運作機制。

12 月份威脅事件阻擋之事件統計表

項次	事件名稱	次數
1	BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283)	**49,958**
2	MALWARE-CNC Win.Trojan.Mudrop variant outbound connection (1:30795)	**5,226**
3	BLACKLIST DNS request for known malware domain browsesmart.net - Win.Trojan.Mudrop (1:30826)	**3,759**
4	BLACKLIST DNS request for known malware domain outobox.net - Win.Trojan.Mudrop (1:30834)	**3,216**
5	BLACKLIST DNS request for known malware domain qualitink.net - Win.Trojan.Mudrop (1:30836)	**2,439**

圖 5　103 年 12 月 Chickenkiller 事件阻擋數約 5 萬筆

```
(c:\windows\system32\nwagent.dll) ----> blogpics.mooo.com Tue Jan 20 12:58:04 2015
(c:\windows\system32\nwagent.dll) ----> freebbs.slyip.com Tue Jan 20 12:59:23 2015
(c:\windows\system32\nwagent.dll) ----> thinkerface.gotgeeks.com Tue Jan 20 12:59:25 2015
(c:\windows\system32\nwagent.dll) ----> facsbook.chickenkiller.com Tue Jan 20 12:59:39 2015
```

圖 5 發現 nwagemt.dll 惡意程式查詢 facsbook.chickenkiller.com

Time Window: 2015-02-01 00:00:00 - 2015-02-28 23:59:00
Constraints: Inline Result = dropped; Impact = Impact 1

Message	Source IP	Count
BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283)		11
BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283)		6
BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283)		4
BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283)		2
BLACKLIST DNS request for known malware domain chickenkiller.com (1:28283)		1

圖 6　104 年 2 月 Chickenkiller 事件阻擋數剩 24 筆

肆、結語

本專案自 103 年 6 月至 12 月共處理 73 件個案，皆已安裝 APT 端點防護軟體進行監控及清除惡意程式。並攔截 APT 郵件共計 14 件。惡意程式後送本府委外防毒案承商製程病毒碼 3 件。透過閘道端防護設備攔截 Impact Level 1 威脅事件(Malware-CNC、Blacklist DNS、Malware-Backdoor)已阻擋 219,449 次，並攔截惡意程式威脅計 2,654 次。本專案所獲得效益如下：

一、 與防毒專案整合發揮加乘效果

(一) 藉由本專案發現受害端點(Server, PC)有 50%以上未確實安裝防毒軟體，故可藉由 APT 事件處理落實本府防毒軟體 100%布建率。

(二) 藉由本專案所擷取的惡意程式可送防毒軟體原廠進一步製成病毒碼並更新防毒軟體，以防止惡意程式的擴散。

二、 藉由本專案加強本府各機關落實處理「國家資通安全會報技術服務中心」通報事件。

三、 整合本府 ISMS、防毒專案 SOC 處理大量事件，以專業廠商的監控服務及處理能量作重點分析處理，以減少大量的人力物力需求。

四、 整合兩家業界領導廠商服務，透過兩家廠商的不同 Know-How 所構織的安全防護網，可更有效的發現 APT 事件或入侵的駭客。

五、 透過本專案所累積的偵防、鑑識相關知識，不管是在整體資安維護、網路管理方面，還是在防毒上都有相輔相成的效果，且可協助各網站、系統主機負責人及各 PC 使用者端提升其系統環境資安防護等級及素養。

本府資訊中心張主任忠吉表示：「智慧政府治理發展是智慧城市的重要一環。面對來自網路的 APT 挑戰，我們希望能做到儘早的發現威脅、即時的事件處理、完整的事件報告，引進國內 APT 防護機制協助我們達成這三大目標，確保市府網路環境和資訊作業平台的安全與穩定，讓各項業務能順利推展。」

參考文獻：

1. APT1: Exposing One of China's Cyber Espionage Units. “Mandiant.” <http://intelreport.mandiant.com/> (accessed 6 March 2015)