學術網路環境內的 APT 攻擊現況之分析研究

侯翔齡　　孫偉哲　　林育漢
行政院國家資通安全會報技術服務中心
shawnhou@icst.org.tw
ray.wzsun@icst.org.tw
guesslin@icst.org.tw

摘要

伴隨網路技術的快速發展，傳統的網路攻擊與入侵模式也隨之不斷地進化，駭客攻擊手法亦由早期非針對特定對象所傳播的病毒感染，慢慢轉變到近年來在資安領域持續受到關注與探討的進階持續性滲透攻擊(Advanced Persistent Threat, APT)。所謂的 APT 在現今的網路威脅中是一種更複雜且更具針對性的攻擊方式，對於攻擊方而言，通常是有組織，有經過訓練的駭客集團；會鎖定特定目標，如政府機關、公司企業、組織機構等，經過長時間佈局與資訊蒐集後，針對其目標利用特定、客製化手法發動攻擊，目的可能包含政治考量、商業利益、宗教立場等因素。

對於當前台灣政府機關而言，APT 毫無疑問是各級網路管理人員必須面對的棘手且迫切求解的課題。本研究即針對在台灣學術網路中曾實地進行鑑識與分析作業的 APT 攻擊實際案例，描述駭客在成功入侵組織內部一台主機後，所可能實行的操作與攻擊邏輯；一開始會搜集相關的系統及網路資訊，而後植入惡意控制程式，不斷地在區域網路內對其他主機進行掃描與擴散入侵攻擊，藉此獲取高價值的隱私資料，進而利用該受到挾持控制的電腦主機做為攻擊其他組織機構的中繼站。祈透過本研究能得知台灣在學術網路當前所面臨的 APT 攻擊其樣態與特性，同時亦可瞭解如何針對學術網路環境進行預防與防護，減低 APT 攻擊所帶來的衝擊與影響。

關鍵詞：網路安全、進階持續性滲透攻擊、針對性攻擊

Abstract

With the rapid development of network technology, traditional network attack and intrusion techniques have been improved. Hacker techniques changed from virus infection targeting non-specific victims to have been widely discussed, the advanced persistent threat. APT is a more sophisticated and highly targeted attack technique among cyber threats. The attackers are usually organized and belong to well-training hacker group who target specific government agencies, enterprises, and organizations. After a long-term incubation and information gathering, attackers developed specific and customized approach to attack targets for political, business or religious considerations.

For Taiwan government agencies, APT absolutely has become one of the most critical and urgent issue which all levels of network managers must face up. This paper describes the actual case of APT we investigated in TANet. According to our investigation, initially, hackers would collect information and inject malicious backdoor programs. Then, they constantly scanning and penetrating other hosts in the same LAN so as to obtain private or confidential data for economic purposes. Finally, the compromised hosts would probably be used as C2 servers to attack other organizations. Throughout this paper, we take a glance of the status and characteristics of APT attack happening in TANet. And we provide suggestions to prevent and defense APT attack as our conclusion.

Keywords: Cyber Security, Advanced Persistent Threat, Targeted Attack

1. 前言

隨著時間的發展，惡意的網路攻擊行為也越趨多元，早期多為透過檔案傳播的病毒感染，而現今的攻擊方式主要為透過縝密的規劃，利用複雜的攻擊手段竊取機密資料的進階持續性滲透攻擊(Advanced Persistent Threat, APT)。在 NISCC(National Infrastructure Security Co-ordination Centre)2005 年的報告[1]中明確地指出，APT 攻擊為一種針對特意選定的組織，在一段時間內利用社交工程(Social-Engineering)郵件植入木馬程式(Trojans)，獲取目標組織的機敏性資料，且這樣的攻擊能有效地躲避傳統的防火牆(Firewall)與防毒軟體(Anti-Virus)的偵測。由趨勢科技(Trend Micro Corp.)於 2013 年所公佈的統計數據[2]，高達 80%的受駭單位並不知道自己遭到 APT 攻擊，且平均要經過超過 300 天才會發覺自己成為 APT 攻擊的受害者，且這些受害單位包含政府機關、科技產業及金融機構等，由此可知 APT 攻擊已成為現今網路安全的重要議題。

本研究試圖透過在台灣學術網路中實際進行事故處理的 APT 攻擊案件，剖析駭客所使用的攻擊邏輯與手法，針對案件中的社交工程郵件、惡意程式樣本及完整事故調查結果，描述台灣學術網路環境中目前的 APT 攻擊現況，最後本研究將提出遭到 APT 攻擊的原因與其改善方法，期望各級的網路管

理人員因此能有效地進行預防與防護，藉此降低 APT 攻擊所帶來的衝擊與影響，增加遭受攻擊時的應變能力。

2. 文獻探討

2.1 APT 定義

APT 攻擊行為也被稱為有長期針對性目標的攻擊，這樣的攻擊行為通常具有一個預先鎖定的目標人物或者是組織，透過長期的蒐集目標資訊並針對目標組織打造量身訂製的攻擊工具，因此 APT 攻擊並不像傳統的惡意攻擊行為可以依靠單一的防火牆或者防毒軟體可以偵測或防範[3]。而 APT 攻擊從政府機關、研究機構以及金融產業等都有可能成為攻擊目標，且 APT 攻擊的潛伏時間從數周至數個月甚至更長，表 1根據 Nikos 等人的研究[4]整理了以下四起自 2007 年以來知名的 APT 案例。

自 2007 年起世界發現多起 APT 攻擊案例，其中 Nikos 等人整理了 Stuxnet、Duqu、Flame 以及 Red October 共四起案例，並且針對這些 APT 攻擊中所使用的惡意程式進行分析，其中發現 Stuxnet 所使用的惡意 APT 攻擊程式複雜度遠超出一般駭客組織所能維護的範圍，除了使用了四個零時差弱點(Zero-Day)的漏洞之外，還需要對於攻擊目標基礎工業流程深入了解，並進行實際破壞攻擊行為。而 Duqu 則是被認為由與 Stuxnet 同組開發人員所開發之惡意程式，與 Stuxnet 相比較多了鍵盤側錄工具，主要攻擊目標也從破壞設施改為竊取資訊。Flame 攻擊所使用的惡意程式與其他攻擊事件相比，檔案大小較大同時具有相當完整的功能，與常見的 APT 攻擊所使用的惡意程式相比較是相當不尋常的。Red October 所使用的惡意程式主要負責與命令與控制主機連線，同時下載各式擴充功能模組，研究發現有超過一千個不同的擴充功能模組，這些擴充模組使得 Red October 的攻擊目標可以相當的廣泛。

表 1. **APT 案例比較列表**

APT 名稱	Stuxnet	Duqu	Flame	Red October
開始攻擊時間	2009 年 6 月	2010 年 10 月	2012 年 5 月	2007 年 5 月
被偵測之時間	2010 年 6 月	2011 年 9 月	2012 年 5 月	2012 年 10 月
檔案格式	DLL	DLL	OCX	EXE
自我散佈途徑	可移除之儲存設備、網路	手動複製	手動複製	手動複製
鍵盤側錄功能	No	Yes	Yes	Yes
攻擊目的	設備破壞	竊取資訊	竊取資訊	竊取資訊

從以上四起 APT 案例中可以看出，APT 攻擊的目的從蒐集機敏資訊到惡意造成實體攻擊不等，且 APT 攻擊的背後通常是由一個駭客組織所構成的，在 Stuxnet 的案例中更可以看到一個 APT 攻擊背後若是有國家組織支援所造成的嚴重影響。

2.2 APT Killer-Chain

一次完整的 APT 攻擊行為，分為許多的階段，而由 Hutchins 等人的研究[5]整理出一套目前 APT 攻擊的概略流程，以利資安人員針對不同階段的攻擊行為作不同的防範。如圖 1 Hutchins 提出的 APT Killer-Chain，將 APT 攻擊分為七個階段，分別從針對攻擊目標的公開資訊蒐集、針對組織製作惡意程式、傳遞惡意程式至目標人物、惡意程式執行、安裝惡意程式或後門程式、獲得主機控制權以及維持惡意程式。

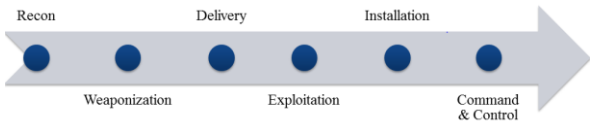

圖 1. **APT Killer-Chain 流程圖**

如圖 2所示 Sean Barnum 等人[6]又將 APT Killer-Chain 從惡意程式執行作為一個區分點，將整個攻擊流程分為 Left of Hack 以及 Right of Hack，來區別 APT 攻擊進行時，從組織外部的情資蒐集到組織內部受攻擊流程。

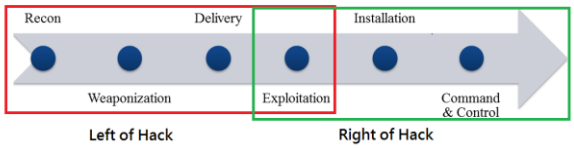

圖 2. **Left of Hack, Right of Hack 示意圖**

藉由這樣的區別，當 APT 事件發生時現場的鑑識人員可以了解並鎖定需要收集之資訊，並且藉由此模型推測攻擊所發生的關鍵點。

3. 事故處理方法

針對資安事故處理，National Institute of Standards and Technology(NIST)提出一套處理流程[7]，而本研究所探討的 APT 攻擊事故調查也採用 NIST 的準則，此章節將會介紹採用的事故處理流程以及所使用的鑑識工具。

3.1 事故處理流程

根據 NIST 所提出的事故處理準則，本研究將完整的事故處理流程細分為 10 個步驟，詳見圖 3，以下將說明各步驟於事故處理的鑑識動作。

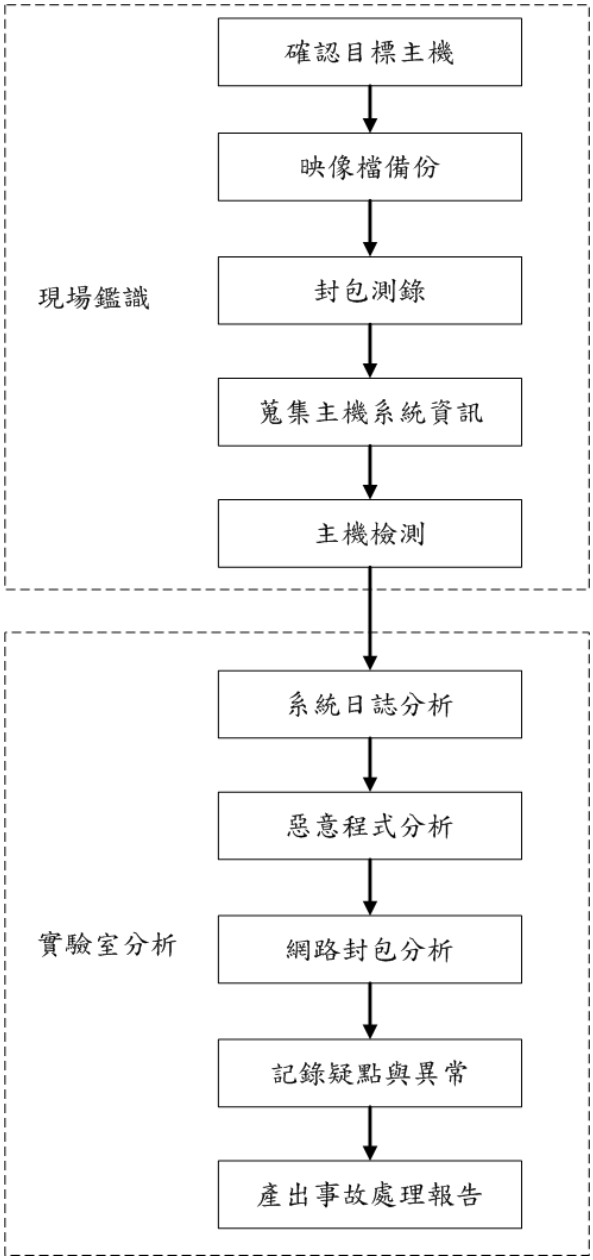

圖 3. **資安事故處理步驟流程圖**

根據資安事故處理的作業環境，可區分為現場鑑識與實驗室分析兩種，現場鑑識主要工作為在現場針對目標主機盡可能搜集完整的資訊，其中包括主機用途、系統日誌、惡意程式及網路封包等，同時處理過程中必須以不變動目標主機中的各項系統組態與檔案資料為前提，避免影響證據資料的正確性；而實驗室分析階段，主要是將現場所搜集到的資料，於嚴格管控且具有專業設備之鑑識實驗室中進行事後分析，彙整所有數位證據的分析結果，產出資安事故處理報告。

現場鑑識的處理流程，首先必須於事故現場詢問管理者有關目標主機的資訊，如主機用途、平時操作狀況。確認目標主機後立即進行 Bits-by-Bits 的硬碟映像檔備份，目的是避免現場事故處理時，各項鑑識步驟不經意地更動目標主機之系統組態，進而影響證據的正確性與完整性。為了找尋可疑的網路連線或是惡意程式的網路行為，因此現場鑑識也必須將目標主機所有的進出網路流量進行封包側錄。當完成上述步驟後即可針對目標主機搜集系統資訊與各類型的系統日誌檔，如：防火牆日誌、防毒軟體記錄、網站日誌及系統事件稽核記錄，同時需要針對目標主機進行全系統的所有檔案進行時間軸記錄，隨後進行目標主機檢測作業，如檢查系統服務(Service)、程式執行行程(Process)、網路連線(Network Connection)等，目的在於第一時間找出可疑的惡意程式或是駭客行為。

結束現場鑑識將所搜集的資料完整帶回鑑識實驗室進行事後分析，運作流程先由系統日誌檔案開始分析，釐清駭客確切的入侵時間、手法及管道，同時確認駭客於目標主機上的行為，再根據駭客的入侵時間，從目標主機映像備份中取得惡意程式，並且進行動態分析(Dynamic Analysis)與靜態分析(Static Analysis)，了解惡意程式的功能用途與行為模式，然後依照網路連線順序將封包重新組合，從中找尋駭客的控制連線指令、惡意程式傳送的加密資料及其他受害者的連線報到記錄。經過上述步驟後，詳加記錄系統日誌中可能的駭客入侵時間與操作行為、惡意程式的功能與用途及網路封包中潛藏的受害者連線與駭客的連線記錄，最後將所有分析的結果，依照時間軸順序詳細載明整起資安事故的過程，產出一份資安事故處理報告。

3.2 鑑識工具介紹

事故處理過程中在不同過程中也將運用不同的工具進行資料分析，表 2會列出我們所採用的各種鑑識工具。

表 2. **鑑識工具名稱與類型列表**

工具名稱	工具類型
FTK Imager[8]	磁碟備份
Sysinternals[9]	主機檢測
Wireshark[10]	封包側錄
Cuckoo Sandbox[11]	惡意程式分析
IDA[12]	惡意程式分析

在現場鑑識作業中，會需要使用磁碟備份、主機檢測及封包側錄共 3 類的工具。在磁碟備份作業中，採用 FTK Imager，針對鑑識目標主機的系統磁碟進行映像檔備份；而為求鑑識過程的系統相容性與穩定度，主機檢測時多以微軟(Microsoft)提供之系統工具 Sysinternals 為主，配合部分自行撰寫之工具，進行主機檢測並搜集所需資料；最後在封包側錄作業時，則是使用 Wireshark 配合網路分流器(Test

Access Port, TAP)來記錄目標主機上所有網路封包，利於後續檢視惡意攻擊網路傳遞之行為。

而在事後的資料分析，將針對現場搜集之系統日誌，利用自行撰寫之工具過濾特定資訊欄位，例如主機的登入成功／失敗記錄或網站的使用者連線記錄，從中判斷是否存在異常。惡意程式分析則需利用動態執行監控方式與靜態反組譯技術，了解惡意程式運作功能與運作情形，其中動態分析主要採用沙箱(Sandbox)測試，所選用的工具為 Cuckoo Sandbox，監控惡意程式運行後所有的動作行為，而靜態分析則是選用 Hex-Rays 的 IDA 反組譯工具，檢視惡意程式內的架構以及運作流程，找出惡意攻擊中所具有固定特徵，藉此彌補動態分析不足之處。

4. 案例分析

本研究整理歸納 2014 年於台灣學術網路環境中的 APT 案件，該機關是位於南部的某大專院校，現場進行事故處理的時間為 2014 年 6 月。經過現場資料、系統日誌記錄、惡意程式、封包側錄各項資料的整合分析結果，推估駭客於此 APT 攻擊事件中各階段的操作行為，以下將以 Hutchins 等人的 APT Killer-Chain 模型，再以 Sean Barnum 所提出的 Left-to-Hack 和 Right-to-Hack 駭客 APT 攻擊模式，詳加描述駭客的攻擊邏輯與手法。

4.1 事故調查分析結果

因有多封政府部門所收到的社交工程郵件，裡面夾帶的附件檔案會產生惡意程式並連線至某南部學術單位的 IP 位址(140.*.*.106)，懷疑該主機已經遭駭客入侵成為連線跳板，因此於 6 月中旬前往進行現場事故處理。

該主機放置於計算機中心的機房內，作業系統為 Windows Server 2003 Standard Edition，主要用途為監控電腦教室各主機網路流量的伺服器。分析調查後，最原始的駭客入侵時間點為 2014 年 3 月，駭客使用「mossadmin」帳號透過網路芳鄰的方式成功登入，其來源 IP 位址為該校園內的另一主機(140.*.*.18)，其入侵過程並未發現駭客試圖以暴力法進行多次登入嘗試，同時根據管理者表示，該帳號的密碼組合並不嚴謹，因此研判駭客事前已取得 mossadmin 帳號的密碼，同時該帳號具有系統管理者權限，因此可透過此帳號控制受害主機。

駭客登入該主機後植入惡意程式 ntmssv.dll，檔案建立時間恰好為成功登入後的 2 分鐘，該惡意程式是一後門程式，運行後會註冊為系統服務，即便系統重開機後依然能運作，同時開啟 1024 通訊埠供駭客操作。駭客陸續透過該後門植入其他惡意程式、建立異常帳號、上傳釣魚網頁及發送大量社交工程信件，以下針對駭客的攻擊行為分別描述。

在此 APT 案例中，駭客利用 ntmssv.dll 後門程式植入 5 個惡意程式，分別為 1 個後門程式(wincomx.dll)、1 個 Port Relay 程式(svchoss.exe)及 3 個密碼竊取(Password Dump)工具(gss.exe、s3.exe 及 wc.exe)，各惡意程式的植入時間與功能描述詳見表 3

表 3. **惡意程式植入時間與功能描述列表**

惡意程式名稱	植入時間	功能描述
wincomx.dll	2014 年 3 月	後門程式，開起通訊埠供其他受害者報到連線，接收駭客的命令
svchoss.exe	2014 年 5 月	Port Relay，具有封包轉送之功能
gss.exe	2014 年 6 月	密碼竊取工具，竊取本機帳號密碼
s3.exe	2014 年 6 月	密碼竊取工具，竊取本機帳號密碼
wc.exe	2014 年 6 月	密碼竊取工具，竊取本機帳號密碼

所有惡意程式經過分析後，其中後門程式 wincomx.dll 運行後，會開啟 3433 通訊埠供其他受害者連線報到，駭客可透過該主機遠端操控連線的受害者，意即該主機已成為駭客控制其他受害者的命令與控制伺服器(Command and Control Server, C2 Server)；駭客利用 svchoss.exe 程式連線多個電子郵件伺服器，如 Google、Yahoo 及 GMX，寄送大量的社交工程郵件；而駭客利用密碼竊取工具，取得該受害主機上所有使用者帳戶及密碼。

檢視受害主機上的使用者列表，發現駭客於 2014 年 6 月新增「admin$」帳號，且曾利用該帳號使用遠端桌面協定(Remote Desktop Protocol, RDP)成功登入主機。

發現駭客於 6 月中旬上傳釣魚網頁，該網頁偽裝成 Google 登入頁面，當受害者連線致該頁面，若誤信為 Google 網站而輸入個人帳號密碼時，駭客將取得該組帳號密碼以及受害者的 Google 聯絡人等隱私資料，而根據網站日誌記錄，發現共有 4 為受害者將自己的帳號密碼洩漏給駭客。

駭客利用釣魚網站所取得的 Google 帳戶，從聯絡人清單中挑選攻擊目標，使用 svchoss.exe 惡意程式，大量發送社交工程郵件，總共發送出 118 封信件，不重複之收件人為 61 位，其中不乏政府機關職員。信件的內容大致可分為釣魚連結和惡意夾檔 2 類，釣魚連結的信件主要都是偽冒成 Google Plus 通知信件，企圖誘騙收件者點選登入自己的 Google 帳號，此時頁面將會導向至駭客先前上傳的釣魚網頁，信件畫面詳見圖 4；駭客將木馬程式嵌入文件檔案中，再寄送給多位收件者，當收件者開啟內含木馬程式的惡意文件檔案時，將會連線至該主機，成為接收駭客控制命令的殭屍電腦。

圖 4. **釣魚連結的社交工程信件內容**

調查結果顯示該主機已成為駭客的 C2 Server，有其他受到駭客挾持的電腦會因此連線報到，於事故調查處理期間有進行封包側錄，時間為期兩周，而從封包中發現總共有 9851 次連線報到記錄，21 位相異的受害者 IP 位址連線至該主機，IP 位址的來源國家為 7 個，受害者來源 IP 連線次數與來源國家詳見表 4。

表 4. **受害者來源 IP 連線次數與來源國家列表**

連線次數	受害者來源IP位址	來源國家
5785	60.*.*.45	台灣(TW)
3983	61.*.*.85	台灣(TW)
11	64.*.*.210	美國(US)
10	36.*.*.40	台灣(TW)
7	84.*.*.45	德國(DE)
6	207.*.*.3	加拿大(CA)
4	128.*.*.57	俄羅斯(RU)
4	188.*.*.12	俄羅斯(RU)
4	188.*.*.180	俄羅斯(RU)
4	193.*.*.231	烏克蘭(UA)
4	46.*.*.232	俄羅斯(RU)
4	66.*.*.253	美國(US)
4	66.*.*.119	美國(US)
4	76.*.*.29	美國(US)
4	91.*.*.227	俄羅斯(RU)
4	95.*.*.249	俄羅斯(RU)
3	85.*.*.19	俄羅斯(RU)
2	176.*.*.163	俄羅斯(RU)
2	72.*.*.112	美國(US)
1	140.*.*.106	台灣(TW)
1	220.*.*.37	中國大陸(CN)

總結整起 APT 攻擊事件，因主機的管理者帳號存在弱密碼問題，因此輕易地被駭客入侵植入後門程式，而產生一連串的 APT 攻擊；而其他受害者則是因為誤信社交工程郵件，導致個人 Google 帳號密碼外流，或是開啟信件中的惡意文件，使電腦遭到駭客植入木馬程式，成為殭屍電腦中的一員。彙整該起 APT 事件的攻擊流程與駭客攻擊行為，其 APT 攻擊流程概念詳見圖 5。

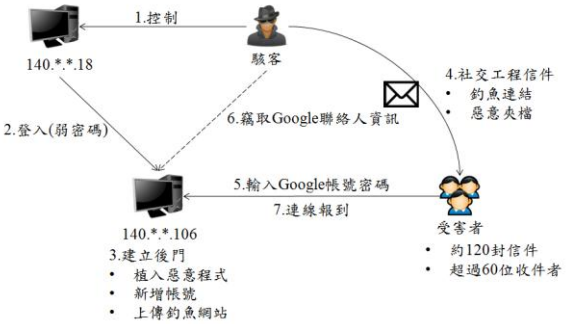

圖 5. **APT 攻擊流程概念圖**

根據 APT 攻擊流程概念圖，將駭客於整起 APT 攻擊案件中所有攻擊手法，依照時間順序細分為 7 個樣態。由於主機(140.*.*.106)存在弱密碼問題，駭客透過先前已取得控制權限之主機(140.*.*.18)登入，登入成功後即建立後門控制程式，並植入惡意程式、新增異常帳號及上傳釣魚網站等行為，目的是為了鞏固駭客于主機上的控制能力以及增加攻擊其他受害者的能量。駭客寄送大量有釣魚連結和惡意夾檔兩大類型的社交工程信件，有收件者誤信釣魚連結並輸入 Google 帳號密碼，將會洩漏露自身的 Google 帳號及密碼給駭客，而當駭客取得 Google 帳號將從中取得聯絡人資訊，並從中挑選下一波 APT 攻擊的目標對象，針對這些目標對象再寄送大量的社交工程郵件，而這些目標對象若開啟郵件內的惡意夾檔，將會連線至該 C2 Serever(140.*.*.106)，成為受駭客控制的殭屍電腦。

4.2 APT Killer-Chain 模型驗證

由於事故處理的對象為一台伺服器，鮮少有收發電子郵件、開啟文件檔案及網頁瀏覽等常見的感染惡意程式行為，因此以該主機的觀點，僅能符合 Right-to-Hack 攻擊模式，但若以收到社交工程郵件

的受害者而言，則是符合 Left-to-Hack 攻擊模式，以下將針對兩種攻擊模式，採用不同受害者的觀點進行駭客行為驗證。

(1) **Right-to-Hack 攻擊模式**

弱點攻擊(Exploitation)：

因為該主機存在若密碼的問題，駭客利用另一主機(140.*.*.18)成功登入，並取得電腦主機的完整管理者權限。

建立後門程式(Installation)：

駭客成功入侵該主機後植入後門程式，遠端操縱此受害主機，並植入其他惡意程式、建立異常帳號、上傳釣魚網頁及發送大量社交工程信件。

命令與控制(Command and Control)：

事故調查處理期間發現 21 位相異的受害者連線至該主機，接受駭客的操縱指令，對於受害者而言，可能會產生令一起的 APT 攻擊事件。

(2) Left-to-Hack 攻擊模式

偵查(Reconnaissance)；

駭客透過釣魚網頁成功取得 4 位受害者的 Google 帳號密碼，藉此獲得其聯絡人資訊，再從中挑選高價值的聯絡人進行下一步攻擊目標。

製作惡意文件(Weaponization)：

駭客將後門程式嵌入文件檔案中，而文件格式選用 Adobe Portable Document Format(PDF)或是 Microsoft Office 為主，當受害者開啟文件檔案將會使自己的電腦被植入後門程式。

傳送惡意文件(Delivery)：

駭客偽冒成釣魚網站受害者的 Google 信箱位址，寄送如通訊錄更新等主旨的社交工程信件，降低收件人的警覺性，提升加附檔中惡意文件成功執行的機會。

弱點攻擊(Exploitation)：

駭客所使用的惡意文件多為 PDF 或是 Microsoft Office 檔案格式，因此利用應用程式的漏洞或弱點植入後門程式，使受害者主機成為駭客可控制之殭屍電腦。

經由兩種受害者角色的觀點，進行 APT Killer-Chain 模型的驗證，發現駭客於受害主機上的攻擊順序，依次為利用弱密碼進行攻擊，攻擊成功後即建立後門連線，此時受害主機已成為駭客的 C2 Server，同時也有更多的受害進行連線報到，這樣的駭客攻擊邏輯符合 Right-to-Hack 的 APT 攻擊模式；若以受害者收到社交工程郵件的攻擊而言，受害者因為自己的電子郵件信箱因釣魚網頁洩漏給駭客，因此駭客寄送良好偽裝的社交工程郵件，同時郵件附檔是遭到植入後門程式的文件檔案，當收件者執行檔案時就被植入後門程式並連線至 C2 Server，而這樣的過程同樣也符合 Left-to-Hack 的 APT 攻擊模式。

5. 結論

經由兩種受害者角色的觀點，進行 APT Killer-Chain 模型的驗證，發現駭客於受害主機上的攻擊順序，依次為利用弱密碼進行攻擊，攻擊成功後即建立後門連線，此時受害主機已成為駭客的 C2 Server，同時也有更多的受害進行連線報到，這樣的駭客攻擊邏輯符合 Right-to-Hack 的 APT 攻擊模式；若以受害者收到社交工程郵件的攻擊而言，受害者因為自己的電子郵件信箱因釣魚網頁洩漏給駭客，因此駭客寄送良好偽裝的社交工程郵件，同時郵件附檔是遭到植入後門程式的文件檔案，當收件者執行檔案時就被植入後門程式並連線至 C2 Server，而這樣的過程同樣也符合 Left-to-Hack 的 APT 攻擊模式。

而根據這次 APT 案例的調查結果，我們提出以下的改善建議供學術網路管理者參考。首先，因為受害主機存在弱密碼問題，駭客因此能夠輕易的入侵，所以我們建議系統上所有帳號的密碼必須符合複雜性原則，例如密碼長度超過 8 個字元且必須包含英文大小寫和數字，同時需要定期地更換密碼，而假若在不同主機上有相通同帳號，其密碼也必須相異，避免駭客取得其中一組帳號密碼即可成功入侵所有系統主機。其次，系統上的系統日誌必須妥善記錄保存，並且定期檢視主機是否遭到異常登入，盡可能在遭到駭客攻擊的初期便能及早發現，阻止駭客後續的攻擊行為。然後關閉主機上不需要用到的服務，以本次 APT 案件為例，因該受害主機的功用僅為監控電腦教室的網路流量，並不需要用到網頁服務，但由於系統安裝後管理者並未主動關閉這項服務，導致駭客利用該主機作為釣魚網頁的站台。因駭客大多仍是透過社工程郵件進行大量散布，所以在個人使用者方面，建議增加資安相關訓練以提升資安意識，避免開啟來路不明的電子郵件與在可疑域名的網站中輸入個人帳戶資料，應能有效地降低成為殭屍網路的機會。

參考文獻

[1] NISCC, (2005, Jun.), “Targeted Trojan Email Attacks”, National Infrastructure Security Co-ordination Centre, [Online]. Available: http://www.cpni.gov.uk/Documents/Publications/2005/2005015-BN0805_Targeted_trojan_email.pdf

[2] 趨勢科技, (2013, Oct.), “2013 年台灣進階持續性威脅 APT 白皮書”,Trend Micro Corporation, [Online]. Available: http://www.trend.com.tw/apt/whitepaper/Trend_Micro_APT_Whitepaper_2013.pdf

[3] G. Kumar and K. Kumar, (2014, Apr.), “Network Security - An Updated Perspective”, Systems Science and Control Engineering: An Open Access Journal, vol. 2, no. 1, pp. 325-334.

[4] N. Virvilis and D.Gritzalis, (2013, Sep.), “The Big Four - What We Did Wrong in Advanced Persistent Threat Detection?”, Proc. of the 8th International Conference on Availability, Reliability and Security, pp. 396-403.

[5] E.M. Hutchins, M.J. Clopperty and R.M. Amin, (2011, Mar.), “ Intelligence-driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.”,

Proc. of the 6th International Conference on Information Warfare and Security, pp. 113–125.

[6] S. Barnum, (2012, Jul.), "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX)," MITRE Corporation, [Online]. Available: http://msm.mitre.org/docs/STIX-Whitepaper.pdf

[7] P. Cichonski et al., (2008, Mar.), "Special Publication 800-61: Computer Security Incident Handling Guide", National Institute of Standards and Technology, [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[8] FTK Imager, "e-Discovery, Computer Forensics & Cybersecurity Software | AccessData",[Online]. Available: http://www.accessdata.com/ (Accessed: Sep. 10, 2014)

[9] Windows Sysinternals, "Windows Sysinternals: Documentation, downloads and additional resources",[Online]. Available: http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx (Accessed: Sep. 12, 2014)

[10] Wireshark, "Wireshark · Go Deep.",[Online]. Available: https://www.wireshark.org (Accessed: Sep. 11, 2014)

[11] Cuckoo Sandbox, "Automated Malware Analysis - Cuckoo Sandbox",[Online]. Available: http://www.cuckoosandbox.org (Accessed: Sep. 12, 2014)

[12] IDA, "IDA: About",[Online]. Available: https://www.hex-rays.com/products/ida/index.shtml (Accessed: Sep. 12, 2014)