網路攻擊來源追蹤技術應用之研究

李志宏
樹德科技大學 資訊管理研究所
changt@mail.stu.edu.tw

李政廣
樹德科技大學 資訊管理研究所
misatocat@gmail.com

摘要

網際網路已成為普遍所使用的通訊環境，TCP/IP 通訊協定中網路上任兩方溝通唯一媒介就是 IP 位址(IP Address)，由於 IP 數量不足的原因，網路服務業者(ISP)對於 IP 之發放採用了浮動 IP 位址的方式，也就是說任何人都可能使用到同一組 IP，任何人在網路上都可保有虛擬匿名的特性；然而，此一方式助長了網路攻擊行為的發生，像是蠕蟲、病毒、阻絕服務(DDoS)的攻擊等。雖然現今提出防禦此類攻擊之各種技術已經非常多且成熟，不過仍然無法完整且有效的找出攻擊的根源。以 IP 位址判斷攻擊來源的依據在 ISP 業者發放浮動 IP 的機制下已經徹底失效。本研究有別於過去對於攻擊只是單純的防禦，主要利用各種 IP Traceback 技術和方法，包含 Link Tasking、ICMP 等，建置一整合性機制以收集攻擊者更多行為線索，藉此採取主動追蹤並定址其網路攻擊來源。此一做法有別於過去對於攻擊只是單純的防禦。

關鍵詞：主動防禦、IP 追蹤、使用者辨識、網路攻擊、整合防禦系統

Abstract

Network has been the one of useful technology in the modern world. IP (IP Address) is the only media in the network form TCP/IP Protocol. Nowadays, ISP use Dynamic Host Configuration Protocol for deliver IPv4's IP address. In another word, every user may be able to use the same IP address at the different time. Therefore any one can keep their identity hidden. However, this way can grow more and more attack behavior by using dynamic to deliver their IP address. The attack such as worm, virus and DDoS (Distributed Denial of Service) are familiar in the network. Even though, a log of way can defense the attack behavior, but has less way can find the attack source and block it. Also, IP address isn't a good clue to identify the attack source. This research wants to bring up a integration way that can identify the source, compared to the old way that only defense the attacker. This research use IP Traceback tools, include Link Tasking, ICMP...ect, to build a system, not only identify the attacker by IP address but also to collect more clue for fund the location of attacker.

Keywords: Actively Defense, IP Traceback, Indentify User, Network Attack, Integration Defense System.

1. 緒論

網際網路所帶來的便利已經成為現代人生活中非常重要的地位。十幾年來，網路應用普及有目共睹，但遺憾的是，網路攻擊的案件也是同比例的增加，從警政署公布的資料顯示，網路攻擊犯罪案件從 2004 年的 14,057 件至 2005 年的 20759 件[1]，成長率竟有 400%以上，因為網際網路其具有的的虛擬特性，使得網際網路成為有心攻擊者的天堂。

網路攻擊意指比較常見的蠕蟲擴散、病毒、阻絕服務、後門程式等等會造成主機資料外洩或軟硬體的實際破壞行為，此類攻擊會造成各種不容忽視、實質上的傷害，不過，好消息是，目前有許多的機制可以有效的防堵網路攻擊，例如運用防毒軟體、入侵偵測系統、防火牆、加密等工具，雖然會花費不小建置的成本，但可確實防犯大部份的惡意駭客攻擊。

另外在使用網際網路行為的觀點上，因網路的虛擬、匿名的特性，很多的網路使用者對於自己的言論不再負責。許多散發不實謠言、中傷他人、詐騙、惡意破壞、干擾網站正常運作等行為，在網路世界形成一種「攻擊行為」。在網站管理人員角度而言，常常會接到此類的申訴案件，輕者刪除使用者，重者報案處理；可惜的是，破案率往往不到 10%。

在 TCP/IP 的協定中，網路上溝通的唯一

代號就是 IP 位址，換言之，能夠辯識使用者來源的依據，就只有 IP 位址；而略過固定 IP 位址不談，目前大多的 ISP 業者因為了讓公司所持有的 IP 更有機動性，發給使用者上網的 IP 多為「動態 IP」，就像出租車一般，在沒有經過規畫的前提下，任何人都有可能「租用」IP 位址，也就是說，任何人都可以以動態 IP 的環境下做攻擊，即使網管人員擋掉攻擊者 IP，只要重新連線，就等於獲得新的身份，繼續扮演著攻擊者的角色；另外，IPv4 在設計特性，攻擊者可以輕易的修改封包表頭的各項欄位，增加追查人員的困難度及不確定性，連帶證據力和證明能力都顯得較為薄弱。

對網路管理人員而言，建置一個完整、安全和乾淨的網路環境可說是最重要工作。所以在網路攻擊頻繁的當下，網管人員就有更多的責任及義務找出攻擊的來源，在攻擊發生時，以最快的速度縮小可疑的範圍，進而找出可疑的電腦，消除攻擊禍源，此實為網管人員新的思考方向。本研究預期開發一套能完整的攻擊追蹤機制，主要使用 Link Tasking 與 ICMP 封包追蹤方法，捨棄以 IP 位址當作主要追蹤線索，主動防禦，以減少因惡意使用者攻擊所造成的傷害。

2. 文獻探討

2.1 IP Traceback

現有安全防護軟體為因應入侵事件而產生的電腦稽核紀錄，大多藉由丟棄(Drop)、停止(Stop)、封鎖(Blocked)、拒絕(Rejected)、終止(Terminated)、拒絕存取 (Access Denied)或攔截(Intercepted)等訊息方式，成功地阻擋已被識別出來的攻擊。這些防護系統所出現的紀錄均為嘗試入侵但未成功的訊息提示，雖未能真正入侵成功，仍然可作為安全防護上的重要參考指標。雖然透過此一方式電腦伺服器就能於事後發現有被入侵破壞的記錄，卻無法推測出自於這些出現未入侵成功訊息的入侵者來源。

IP Traceback 即是提出一種方法，找出攻擊封包來源並且終止攻擊的方式，此一概念最早是由 Stefan Savage 等人所提出之 Practical Network Support for IP Traceback[1]，最主要用於找尋並防止 DDoS(Denial Of Servic)和 IP 欺騙(IP spoofing)兩種網路上常出現的攻擊。

目前，常見的 IP Traceback 的方法有：Link tasting、Logging 和 ICMP Traceback(iTrace)，三種方法，以下分別簡介：

2.1.1 Link tasting

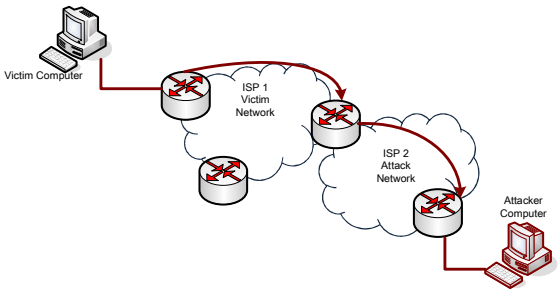

圖 1. Link Testing

Link testing 為一種循序漸近的測試方式，如圖 1 所示，由受害者為出發點，測試所有上游連線，重覆步驟，循序向上追朔，直至發現攻擊來源。目前 Link Testing 又分為 Input debugging[5]及 Backflooding 兩種測試方法。

目前所使用的路由器大部份具有 Input debugging 功能，讓管理者可用於禁止一些特定的封包進出來管理網路，也可檢測出特定封包是由那一個界面(Interface)進入，而此特性可以用於路由的反向追蹤。其缺點是在多個 ISP 之間協調是件費時費力的工作，在實際運作上不能保證所有的 ISP 都會願意合作。

2.1.2 Logging

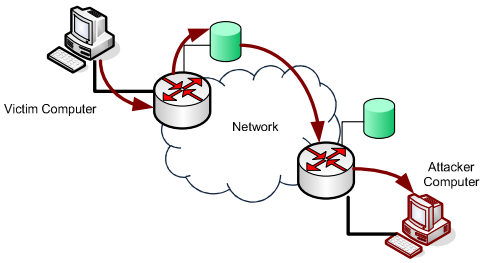

圖 2. Logging

Logging 法是在路由器中紀錄所有經過的封包資訊，如圖 2 所示，所記錄的資訊可包括來源位址、目的位址及封包數量等資訊。這些資訊保留在各端口的路由器中，當攻擊發生時，受害者可由路由器中找到其紀錄或封包所共有的特徵，以此為線索向上追查，在各個路由器的紀錄中查訪和比較，進而比對出攻擊路

徑。此方法優點在於攻擊事件發生後可以容易處理並且具公信力，但路由器需要儲存及處理大量的資料並且需要資料庫技術來加以支援。

以上提及紀錄封包的方法並不完善，它存在著下列幾個問題。首先，因為路由器的儲存空間有限，所以一旦其儲存空間飽和，其相對應之攻擊路徑資訊就無法紀錄，即會影響其追蹤攻擊者的能力；再者，由於其對應方法乃是利用雜湊值，會有碰撞的情況產生而誤判攻擊路徑；另外，各路由器必須在其上增加數百萬位元組記憶空間，成本上不太實際；最後，以路由器去尋找一封包相對應的位元是否存在，這項工程相對於路由器本身的處理能力實在太過於沉重。綜上所述，以及核心路由器(Core Router)一天經過的封包數量實在過於龐大，我們可以看出要以路由器紀錄所流經封包來追蹤攻擊者實在不是一件簡單的事情。

2.1.3 ICMP Traceback(iTrace)

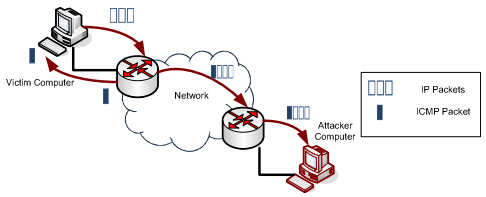

圖 3. ICMP Traceback

ICMP 傳訊封包追蹤攻擊位置的技術，當攻擊者發動攻擊時，其所發出的封包經過配合的路由器，該路由器即會發出相對於該封包的ICPM 封包至其封包所欲到達之目的地。因此，一個攻擊封包會對應到數個 ICMP 封包，至於其所對應的個數量，則取決於該攻擊封包所經過配合路由器的數量。

藉由 Bellovin 領導的 ICMP 協定推展小組，提出了另外一種方法，該演算法需要利用有支援追蹤機制的路由器，稱為 iTrace[6]路由器，一個由路由器以機率 p 發出的一特殊形式的 ICMP 封包，其封包包含發送此封包的路由器位址，以及該封包所經過的上一個路由器和下一個路由器的 IP 位址。如圖 3 所示，iTrace 路由器傳送一 ICMP 封包給該封包之來源和目的位址之主機。

然而，這樣的做法有一致命的缺點，就是其所發出的 ICMP 封包數量是數倍於原始攻擊封包。也就是說一旦攻擊者利用該項特性發動 DoS 攻擊，則攻擊者只要花費原來攻擊的數分之一的力氣，即可以癱瘓其攻擊目標之網路頻寬及電腦。為節省追蹤攻擊者所產生的封包數，可以結合封包登入和傳訊使得發出封包的數量可以減少，也可減少路由器儲存封包資料的空間。

然而，要將這些註記資訊放在封包中的什麼位置是比較恰當的，這就是一個很大的問題。首先，若是每個經過的路由器都要將其 IP 位置放進封包內，一個封包從來源端至目的端經過的路由器最多不會超過 30 個。也就是說在 IPv4 中我們必須將 60 位元組的資訊放進封包內，因為表頭的長度不夠，所以就必須要把這些追蹤資訊放入經過封包的 Payload 中。然而這樣會造成兩個很嚴重的問題，可能會因為加資料在原來封包中，造成原來封包變大而需要對這封包做切割。最嚴重的就是，路由器沒有辦法承受我們將資料插入每個封包的 Payload 中這麼重的負擔，因此大部分封包標記的方試都將附註資料記錄在路由器原本就要處理的 IP 表頭內，如首次由 Burch 提出的隨機封包標示(Probabilistic Packet Marking)，Savage 並於 2000 年討論封包標記這類型實作時所需考慮之技術細節。因為目前要傳送封包之前都會先找出路徑中的最大傳輸單位(Maximum Transmission Unit, MTU)，所以只有 0.25%的封包會在封包送出後做切割(Fragmentation)。所以這方法讓路由器依著機率在封包 IP 表頭之識別欄位上面，寫上自己的 IP 位址。一旦攻擊封包穿過合作的路由器，受害者端就可用收到的封包建構出攻擊路徑。若是所有的邊界上路由器都已經支援追蹤攻擊者的這項功能，只要在封包要進入網際網路時打上註記，其他中繼的路由器都不需要再打註記。一旦攻擊發生就把這些攻擊封包所在註記的位置解譯出來即是攻擊來源，相對地追蹤攻擊者也就變得容易許多。

2.2 Cookie

2.2.1 Cookies 概述

所謂 Cookies 就是當使用者瀏覽某個網站時，該網站在使用者的電腦中所儲存的一小段資訊，該項資訊可能以文件的型態儲存在硬碟中，或是暫時儲存在記憶體中。伺服器可將有

關客戶端的一些相關資料設定到客戶端的硬碟當中，以便當下次客戶端再度連線進入 Web 網站時能夠藉由此條連線所攜帶的資料進行處理，而其中一個重要的應用就是在電子商務上，尤其是網路購物。例如將客戶的姓名記錄在 Cookie 中，當下次客戶再度連線時直接攜帶此 Cookie 姓名資料進入網站，就可直接顯示出顧客姓名於首頁畫面，不需使用者作任何 Key In 的動作。其實，這樣的 Cookie 資訊可得到一個非常好的優點，那就是將一些非機密性的資料記錄在客戶端上，客戶連線時攜帶此 Cookie 資料直接提供 Web 網站使用，可節省許多客戶輸入這些資料的時間。

又如亞馬遜書店(http://www.amazon.com)的系統會分析客戶的偏好，根據客戶的偏好，在該客戶連上 Amazon 的網頁時，系統會製作出一頁客製化的網頁，因此不同的客戶會有不同網頁的呈現，這些都需要透過 Cookies 來完成。

除了個人化的目的外，Cookies 另一個目的是儲存使用者個人資訊，簡化使用者認證的程序，有些網站要求使用者必須先註冊後才能使用該網站，為了簡化使用者登入的程序，網站會將使用者的資訊紀錄在 cookie 中，例如 IP、Password 等，使用者再次登入時，可省去輸入 ID 與 Password 的手續直接登錄。

2.2.2 cookies 的結構

以下列出當在 PHP 語法使用 cookie 語法時，會使用的結構名稱及參數。

- Name:指定 Cookies 的名稱
- Expires:指定 Cookies 資料的有效期限
- Domain:指定可以存取該 Cookie 的網域 (表 1)
- Path :指定可以存取該 Cookie 的路徑 (表 2)
- Secure :值域為 True 或 False，代表 Cookies 資料是否以 SSL (Secure Socket Layer) 的方式傳送

2.2.3 Cookies 的應用

Cookies 的應用分類如下：

- 身分識別：採用會員制的網站可藉由存取使用者端電腦的 Cookies，迅速辨認出會員身分，讓使用者快速登入網站。
- 客製化網站：當使用者進入某一特定網站時，希望只要接觸到部分種類的內容或是功能就好，透過 Cookies，使用者可自行設定要出現哪些內容或是功能。
- 網站追蹤：對於網站管理者來說，可經由存取 Cookies，追蹤使用者瀏覽過哪些網頁，進而分析出使用者偏好於哪類的內容，針對該部進行加強的工作。
- 歷史紀錄：對於已瀏覽過的內容，例如新聞網站的新聞或是搜尋引擎所搜尋出來的網頁，會將已瀏覽過的部分加以標記，避免浪費時間於閱讀同樣的資訊或是重複瀏覽已查過資料的網站。

2.2.4 Cookies 的性質

前面提到 Cookies 可能為文件的型態儲存在硬碟中，或是暫時儲存在記憶體中，因此可以得知 Cookies 可分為暫時性與非暫時性的；所謂暫時性的 Cookies，是指在瀏覽器工作階段所暫時需要保存在電腦上的資訊，這類的 Cookies 會隨著瀏覽器的關閉，自電腦中刪除；與其相對，非暫時性的 Cookies 就是指，即使瀏覽器關閉，這份資訊也不會消失，並以檔案的型態存在電腦磁碟中，當使用者再次連到該網站，這份檔案就可再度被利用，而 Cookies 存在時間的長短是由網站的程式所設定。

2.3 工具簡介

2.3.1 IP database

2.3.1.1 TWNIC

財團法人台灣網路資訊中心(TWNIC)是一個非營利性質之財團法人機構，同時也是中國互聯網絡信息中心(CNNIC)、日本網路資訊中心(JPNIC)、韓國網路資訊中心(KRNIC)等網際網路組織之對口單位。

其中，TWNIC 提供了網域名的查詢和登記的功能，在於查詢功能上，可供使用者能透過介面程式查詢特定 IP 的基本資料，其中包含了IP所註冊的機構名稱，機關和所屬的國家(如圖 4)。近年來已成為國內查詢 IP 資料的重要工具網站。

查詢功能-IP/ASN查詢

IP代理發放單位網段:210.71.0.0-210.71.127.255	
Chinese Name	教育部
Netname	TANET-NET
Organization Name	Ministry of Education Computer Center
Street Address	12F, No 106, Sec 2,Hoping E. Rd.,
AdminHandle	YHC153-TW
TechHandle	TA8-TW
SpamHandle	YHC153-TW
用戶單位:210.71.4.0/22	
Netname	T-STU.EDU.TW-NET
Organization Name	Shu-Te University
Registered Date	1998-09-02
Admin. Contact	abuse@mail.stu.edu.tw
Tech. Contact	abuse@mail.stu.edu.tw

圖 4. Twnic

2.3.1.2 GeoIP

除了使用上所述的三種 IP Traceback 技術之外，在所服務伺服器建置完整的資料庫，可以更快速鎖定和追蹤使用者，Maxmind.com 所提供的GeoIP是一整合全球IP使用資料並且以資料庫的形式提供於網路使用者，此一完整的資料庫整合的資料可以定義出每一個 IP 所屬 ISP、公司名稱、國家及城市。

此一資料庫主要提供於網頁伺服器架設的使用者，可用於封鎖或限制某一國家或某一城市的使用者，由 GeoIP 所提供的資料庫，依所取得的層級不同，所能得到詳細的資料不盡相同，但準確度可高達 97%。

3. 研究方法

3.1 系統架構

為了有效阻止入侵或是攻擊事件的發生，以及達到防禦且主動追蹤主要目地，在況狀發生時收集所有可得線索，講求整體流程策略的的最佳效率，本論文使用了 cookie 當做使用者標記方式和 ICMP Traceback 來達到鎖定追蹤使用者實體位址的目標。

本章節將說明 IP 位址追蹤系統架構，以及各系統設計概念及原理，分別就入侵偵測、自動(手動)鎖定、收集線索、追蹤流程，說明系統設計概念以及各系統之運作原理。接下來，把本研究所提出的應用系統結合目前網際網路業者所提供浮動 IP 做討論，提出浮動實體 IP 位址的整合解決方案。

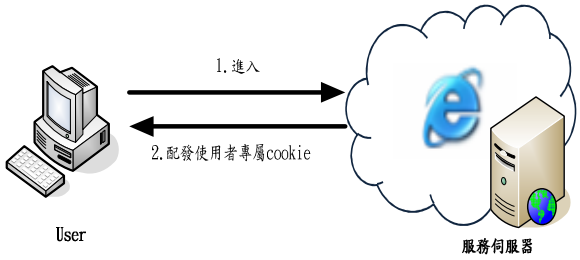

圖 5. 系統架構圖

3.1.1 使用者標記

圖 1 是本研究的系統架構圖。正常的瀏覽的情況之下，使用者在進入網站進行服務時，網頁伺服器會自動在每個使用者的電腦上配發一組由亂數產生獨一無二內容的 cookie，本系統的 cookie 建立方法是利用 PHP 程式 srand ((double) microtime() * 10000000)產生一種亂數，做為本系統瀏覽者的 cookie 值，而系統也將 cookie 存活期限預設為一年。當正常從事瀏覽行為時，系統對於使用者的處理也僅止於此。目的在於每個使用者不管是在使用靜態網頁或是動態網頁服務時，系統會主動配發一組 cookie，使得系統可以判斷並紀錄每位使用者，像是運用在討論版時，可在發言同時在後端處理時紀錄此發文者的 cookie 值，如此一來，即使在不知道使用者帳號的情況下，也可以鎖定使用者所使用的電腦。

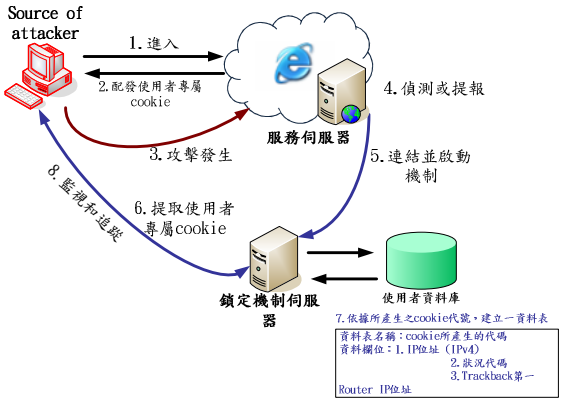

圖 6. 攻擊發生，啟動鎖定及判斷機制

3.1.2 異常狀況偵測和判定

圖 2 是目前網路上有攻擊發生，此時系統管理者可依照系統所發出的 cookie 紀錄啟動鎖定及排除使用者的機制，鎖定機制伺服器依照

所發文紀錄的 cookie 代碼為依據，在資料庫中建立以此代碼為名的資料表，此資料表最主要的功用在於紀綠攻擊者每一次上線時所使用的包含 IP 位址、使用瀏覽器名稱、OS 和需設語系等相關各種資料，此做法有點像是搜證系統，目的在於攻擊者的資料收集越多越好。

3.1.3 監視和追蹤

即至目前為止，所收集到攻擊者的資料僅止有 IP 位址、瀏覽器和 OS 等資料，此資料提供了攻擊者的一些基本資料，也稱之為初步的線索，在攻擊發生當下，依其此線索，將資料所示的 IP 位址帶入系統中 Perl 程式，帶出其 IP 的使用資料，再著使用另一組 Perl 程式，利用 Link tasting 的方式，追蹤攻擊路徑，並且依其記錄至資料庫中。

現今的網路架構中，使用 Link tasting 作為追蹤路徑，在於 Router 設定的限制下，往往只能呈現不完整的 IP 路徑，若是遇到此情況，系統將會改用 ICMP 封包追蹤，同樣也是使用 Perl 來實現其技術，但此技術因 ICMP 封包會消耗掉大量的系統資源，在於系統使用的決策上，以 Link Tasting 為主。

3.2 浮動 IP 的解決方案

現今的網路服務業者(ISP)，對於 IP 的發送大多採用動態的方式，換言之，使用者在於每次使用 PPPoE 連線網路時，所取得的使用 IP 皆有所不同，此一類似於 DHCP 的發送使用 IP 的方式，在於 IP 不足的情況下，可以減少 IP 使用上的浪費，但往往造成其他的問題，使用者因為 IP 的不固定性，使用心態上也出現了微妙的變化，從使用者轉變成惡意的攻擊者時，所使用的 IP 不固定往往造成被攻擊的管理端在於封鎖和追蹤極大的難度。

網站或服務遭受攻擊時，雖然可以很輕易的發現來源的攻擊 IP，對於封鎖和防禦相對簡單，不過一遇到了浮動的 IP，相對難度也爆增不少，只要攻擊端重新連線或使用更新 IP 的方式，又跟善良的網路使用者沒什麼兩樣，相同的攻擊又會發生，所幸，ISP 配發確實有規則可尋，同一地區所配發的 IP 位址大至上都會有個範圍，以大台北地區而言，一個區以一組 Class B 來隨機配發 IP 位址，這提供了網路管理者一個封鎖的依循，可以依照攻擊者來源 IP 來推測此攻擊者大致使用那些範圍的 IP，再者在系統內使用 Mask 的方式封鎖特定範圍的 IP，來達到防禦攻擊的目的，但是此方法可謂「治標而不治本」，以 Freebsd 中 rc.firewall 防火牆的設定方式(如圖 7)，可以發現此方式是把整個 Class C 的 IP 全部封鎖，一方面達到防禦目的，另一方面確同時讓 256 組(人)無法進行服務。

```
#UnTrust_IP1="61.31.128.0/24"
#UnTrust_IP2="219.80.128.0/24"
#UnTrust_IP3="220.163.0.0/16"

#$fwcmd add 00120 deny ip from
${UnTrust_IP1} to me
#$fwcmd add 00121 deny ip from
${UnTrust_IP2} to me
#$fwcmd add 00122 deny ip from
${UnTrust_IP3} to me
```

圖 7. Freebsd 中的 rc.firewall 部份設定檔

ADSL 已成為國內非常普遍的上網方式，但是 ISP 的 IP 發放方式成為了惡意攻擊者的利器，換言之，以 IP 作為攻擊來源的依據已經澈底失效，不論是防禦或是追蹤攻擊端，以此網路架構下，需要另一種更可靠的防禦和追蹤方式，本研究提出了一種類似數位證據收集的方式，把目標從鎖定 IP 改為鎖定電腦的方法，在使用者每次使用服務時，使用 Cookie 的方式在使用者電腦種下可提供線索的種子，內容紀錄了像是使用者國家、使用 OS、瀏覽器甚者每次上網所使用的 IP 位址，有需要時，提供了非常好的線索，透過本研究所提出的系統分析，在攻擊當下可以追蹤至攻擊端的位置，進而紀錄攻擊者和防禦。

3.3 系統架構與系統實作

本研究建置一前端服務，目前建置一以 PHP 所寫成的留言版面供使用者使用，此程式目前可依據使用者上站時間、所使用 IP 做紀錄，並且發放一組 cookie 給其使用者，圖 8 展示程式基本樣式，圖 9 為內部所紀錄使用者的來源 IP。

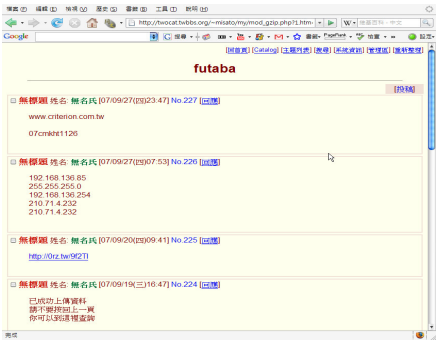

圖 8. 服務介面

圖 9. 管理介面

在追蹤機制上，可以依照系統所紀錄之內容進行初步的鎖定，以 IP 為基礎做第一次的追蹤，使用 GeoIP 所提供的全球 IP 資料庫，如圖 10 查詢其 IP 的基本資料。

Hostname	Country Code	Country Name	Region	Region Name	City
192.72.80.36	TW	Taiwan	03	T'ai-pei	Taipei

圖 10. IP 查詢結果

無關準確率與否，此一數據對於追蹤者已有基本的資料，在 ISP 每次都被發同一人不同 IP 的情況下，系統對於攻擊者每一次查詢所得的紀錄會逐一存入資料庫中作為線索，此一動作可得知攻擊者每次所使用 IP 的區間為何，對於封鎖的規則上很有幫助。

接下來，使用 Link Testing 的方式查詢來源所經過的路徑，設法找到上遊的攻擊來源(如圖 11)，此例而言，所查詢的是一組 Seednet 所使用的 IP 位址，在初步查詢時即可得知此 IP 是在台北所使用，在第二階段的 Link Testing，所測試所得的結果，可以發現路徑追查至 IP 位址為 192.72.80.4，再依照 Seednet 的機房配置機制，很容易的可以定義出使用此 IP 位址設備實體位址，換言之，攻擊者是使用並經由此 Router 的設備發送封包，進而可以把攻擊者鎖定在同一個區域中。

```
traceroute to 192.72.80.36 (192.72.80.36), 64 hops max, 40 byte packets
 1  FDRY1500-bb2 (210.71.23.126) 0.542 ms  0.398 ms  0.359 ms
 2  NS5200 (210.71.22.254)  2.103 ms  2.592 ms  3.361 ms
 3  mi10i-wan (210.71.22.126)  2.731 ms  3.091 ms  2.485 ms
 4  140.127.160.237 (140.127.160.237)  3.482 ms  1.308 ms  1.456 ms
 5  * * *
 6  R122-225.seed.net.tw (192.72.122.225)  13.109 ms  9.782 ms  9.727 ms
 7  R58-153.seed.net.tw (139.175.58.153)  9.725 ms  9.593 ms  9.722 ms
 8  R59-19.seed.net.tw (139.175.59.19)  9.982 ms  9.578 ms  9.731 ms
 9  L4SW-tpemail.seed.net.tw (192.72.80.4)  9.730 ms  12.668 ms  12.601 ms
```

圖 11. Link Testing Traceback

4. 結論與未來研究

目前，整個網際網路依然還是使用 IPv4 技術為主要的傳輸環境，在 IPv6 還沒普及前，各種類似於 DHCP 和 NAT 等為因應 IP 發放不足技術也日漸成熟，但相對對於 IP 是否可以用於辨識單一使用者也顯得越來越困難，網路管理者對於資訊安全的態度轉向防禦，使用各種可靠的技術防止攻擊，然而這卻無法有效的根治攻擊行為。

本研究所開發的系統以求在於快速的追蹤攻擊者，以求達到主動防禦的目的，面對現行 ISP 發放 IP 位址的方式，本研究不單單只依靠單筆 IP 位址來做為追蹤線索，而是把目標放在攻擊者的電腦上，使用各種方法和工具，來實現此系統追蹤攻擊者的能力。

未來本研究對於 IP Traceback 的技術希望能再對於效率上再做提升，例如 ICMP 使用於 IP Traceback 的效率研究，另外一方面，目標也放在於精準的判斷使用者的實際位址，即使利用最少的線索，也可快速且精準的追蹤鎖定攻

擊者位址。

參考文獻

[1]內政部警政署警政治安全球資訊網，2004年，***http://www.npa.gov.tw/***

[2]A. Mankin, D. Massey, ***"On Design and Evaluation of "Intention-Driven" ICMP Traceback"***, IC3N'2001, Oct 2001.

[3]H. Aljifri, M. Smets and A. Pons ***"IP Traceback using header compression" Computers & Security Vol22***, No 2, pp 136-151, 2003

[4]M. Muthuprasanna, G. Manimaran, M alicherry and V. Kumar, ***"Coloring the Internet: IP Traceback"***, IEEE 0-7695-2612-8/06, 2006

[5]R. Stone, ***"CenterTrack: An IP OverlayNetwork for Tracking DoS Floods"***, Proc. 9thUsenix Security Symp., Usenix Assoc., 2000,pp.199-212.

[6]S. Bellovin, ***"Internet Draft: ICMP Traceback Messages"***, Aug 2003.

[7]S. Savage, D. Wetherall, A. Karlin and T. Anderson ***"Practical Network Support for IP Traceback"***, ACM 1-58113-224-7/00/0008, 2000

[8]S. Savage, D. Wetherall, A. Karlin and T. Anderson ***"Network Support for IP Traceback"***, IEEE 1063–6692/01, 2001

[9]Y. Jing, P. Tu, X. Wang, G, Zhang ***"Distributed-Log-based Scheme for IP Traceback"***, IEEE 0-7695-2432-X/05, 2005