開放性 DNS 解析伺服器之防治

謝木政　　陳怡碩
國立清華大學　計算機與通訊中心
{ mucheng, yschen }@cc.nthu.edu.tw

摘要

近來網際網路上為數眾多且設定不當的開放性 DNS 解析伺服器遭利用來發動分散式阻斷服務攻擊事件逐漸增多，然而多數使用者未必知悉其電腦設備遭利用成為網路攻擊事件中的幫兇。為了消除校園網路可能潛伏這類攻擊的打手，確認上網設備是否為開放性 DNS 解析伺服器，進而協助使用者修正設定有其需要。本文以校園網路維運中心的觀點，探討防治開放性 DNS 解析伺服器的作法，同時提出一個快速尋找校園網路內開放性 DNS 解析伺服器的方法，由即時分析骨幹路由器的流量資料，找出可能的 DNS 伺服器 IP 位址，再經過設置在校園網路外的檢測器判定是否為開放性 DNS 解析伺服器，此方法已經過實作的偵測系統驗證其有效性。

關鍵詞：開放性 DNS 解析伺服器、分散式阻斷服務、網路管理、流量分析。

Abstract

The events of DDoS attacks, which are made by a huge number of misconfigured open DNS resolvers on the Internet, have increased recently. However, most administrators of these resolvers did not know that their devices might help these attacks. In order to remove such open DNS resolvers from the campus network, first to locate them and then to help their administrators fix the wrong configurations are demanded. Based on the viewpoint of campus network operation center, this paper discusses how to fix the open DNS resolvers and also presents an efficient approach to detect the open DNS resolvers inside the campus network. The procedures are to find the IP address of the possible DNS server first via real-time analysis of the NetFlow data of the core router, and then to identify it via the detector located outside the campus network. And the effectiveness has been verified by an implemented detection system for open DNS resolvers.

Keywords: open DNS resolver, DDoS, network management, NetFlow.

1. 簡介

DNS(Domain Name System) [1]為網際網路服務中最重要的基礎建設之一，凡上網的電腦設備皆須用到 DNS 伺服器來查詢連線主機的 IP 位址、網域名稱等各項資源記錄(resource record)，方能享用網際網路的便利性。由於近來利用 DNS 的攻擊方式－DNS 反射攻擊(DNS reflection attack)或稱 DNS 放大攻擊(DNS amplification attacks) [2]－已經從理論探討逐漸變為事實夢魘，相關事件日益增多，其中最引人注目的案例莫過於今年 3 月反垃圾信組織 Spamhuas 遭受史上破紀錄 300 Gbps 的分散式阻斷服務(DDoS)攻擊[3]，根據 CloudFlare 分析這次事件[4]，至少有三萬台以上開放性 DNS 解析伺服器(open DNS resolver or open recursive DNS server)參與攻擊，即使每台僅提供數 Mbps 的流量，集滴成川，滙成百 Gbps 巨流，沛然其勢莫之能禦，不僅癱瘓 Spamhaus 網路，全球有數百萬網路用戶亦受到波及。這類攻擊利用原本已遍佈全球各地之設定不當的開放性 DNS 解析伺服器做為打手，對一個有上萬台以上電腦使用的校園網路環境，使用者們對電腦網路技術的熟悉程度有別，難免因設定不慎或軟體預設等問題而造成可資攻擊者利用的機會。再者，這些月來筆者由維運的校園 DNS 伺服器使用記錄，觀察到某些異常巨量查詢的校園用戶 IP 位址，經檢測確認其中部分具有開放性 DNS 解析伺服器的問題，而當事人多半不了解問題所在，因此，筆者撰寫本文希望能協助校園網路使用者了解開放性 DNS 解析伺服器的相關知識，進而避免其管理設備淪為網路攻擊事件中的打手。

要了解開放性 DNS 解析伺服器的問題，首先要知道 DNS 記錄之解析過程(resolution) [5, 6]，以圖 1 為例，當一部用戶電腦(client)要查詢 www.nthu.edu.tw 的 IP 位址，期望所指定的 DNS 伺服器能代為查得最終答案，故對其送出具有遞迴要求(recursion desired)的 DNS 查詢網路封包(如圖 1 中標示為步驟 S1，主要用目的通訊埠 udp/53)，而這部提供遞迴查詢(recursive query) 服務，負責解析 DNS 記錄，找到最終答案的 DNS 伺服器就稱為遞迴名稱伺服器(recursive name sever)。首先，遞迴名稱伺服器以委託問題向 root 名稱伺服器查詢(步驟 S2)，但因 www.nthu.edu.tw 並非註冊在 root 名稱伺服器之上，故介紹它去問可能更接近答案的下一層授權 tw 名稱伺服器(步驟 S3)；重覆對下一部名稱伺服器進行相同問答程序，直至找到該查詢問題的

授權 nthu.edu.tw 名稱伺服器，獲得最終答案為止(步驟 S9)，最後回應用戶答案(步驟 10)。另外，遞迴名稱伺服器為了加速回應已查詢過的 DNS 記錄，通常將之暫存在本機的快取(cache)上，保留該記錄的 TTL 時間(time-to-live)過後才清除，故又稱此伺服器為快取名稱伺服器(caching name server)。圖 1 右方的授權(authoritative)名稱伺服器，由 root 開始，分層授權給以下各授權名稱伺服器負責註冊其授權區域(zone)內最新、最正確的各項 DNS 資源記錄，如：A (IP 位址)、MX (郵件交換器)、NS(授權名稱伺服器)等，故須開放網際網路上任何用戶查詢其授權範圍內的 DNS 資源記錄。圖 2 為用 dig 指令來呈現上述 DNS 記錄解析的過程，由 root 依序看到每一層授權名稱伺服器的回應結果，每一層皆有數部以上授權名稱伺服器 (圖 2 中回答僅列部分 NS 記錄)，以維持 DNS 運作的穩定。

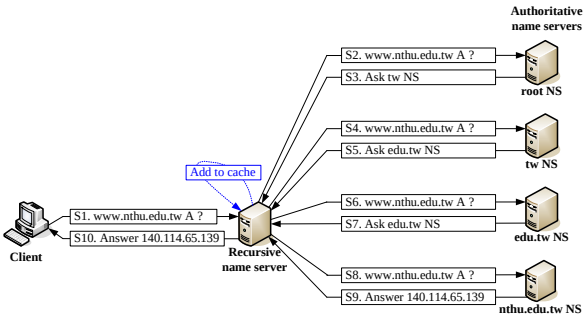


圖 1. DNS 記錄解析過程

```
# dig +trace @140.114.xx.1 www.nthu.edu.tw

; <<>> DiG <<>> +trace @140.114.xx.1 www.nthu.edu.tw

.       106875   IN      NS      a.root-servers.net.
.       106875   IN      NS      e.root-servers.net.
略…
;; Received from 140.114.xx.1#53(140.114.xx.1)

tw.     172800   IN      NS      a.dns.tw.
tw.     172800   IN      NS      b.dns.tw.
略…
;; Received from 198.41.0.4#53(a.root-servers.net)

edu.tw.   86400   IN      NS      c.twnic.net.tw.
edu.tw.   86400   IN      NS      d.twnic.net.tw.
略…
;; Received from 203.73.24.8#53(a.dns.tw)

nthu.edu.tw.  300   IN      NS      dns2.nthu.edu.tw.
nthu.edu.tw.  300   IN      NS      dns3.nthu.edu.tw.
略…
;; Received 251 bytes from
168.95.192.10#53(c.twnic.net.tw)

www.nthu.edu.tw.  86400  IN   A    140.114.69.135
nthu.edu.tw.      86400  IN   NS   dns2.nthu.edu.tw.
略…
;; Received from 140.114.63.10#53(dns2.nthu.edu.tw)
```

圖 2. 以 dig 指令呈現 DNS 記錄解析過程

了解 DNS 記錄解析的運作原理後，接著說明何謂「開放性 DNS 解析伺服器」，根據[7]的定義為 DNS 伺服器提供其管理網域範圍外的用戶，開放使用 DNS 遞迴查詢權限的服務(也就是幫任何人查任何 DNS 資源記錄)，這將產生以下這些問題：

1. 易遭外界濫用，而造成電腦系統與網路頻寬不必要的資源浪費。
2. 易遭有心人士對 DNS 伺服器的快取資料下毒(cache poisoning) [8]，置放錯誤的 DNS 記錄，造成使用者被誤導而連線到有害的地方，例如假冒的銀行網站 IP 位址。
3. 易遭攻擊者利用假造來源的 IP 位址，成為 DDoS 攻擊的幫兇，造成重大網路事件。

理想上要從根本解決這類 DDoS 攻擊的發生，網際網路上須做到徹底杜絕假造來源 IP 位址的封包流通，或是消滅所有網路上的開放性 DNS 解析伺服器，但現實上這兩項工作須要所有網路提供者與設備配合才行，範圍太廣、數量太多、難度太高，目前有 Open resolver project[9]在努力倡導中。不過，縮小範圍以校園網路維運中心管理者的觀點，消除一個校園網路內開放性 DNS 解析伺服器是可行、可努力的目標，基於我們先前防治開放性郵件中繼(open mail relay)以避免助長垃圾信氾濫的相同理念[10]，本文重點在如何消除校園內開放性 DNS 解析伺服器，避免助紂為虐，而不在於如何防禦 DDoS 攻擊。因此，我們運用校園網路骨幹路由器的網路流量資訊 NetFlow[11]，發展一套自動偵測開放性 DNS 解析伺服器的系統，以快速有效地找出校園內開放性 DNS 解析伺服器的 IP 位址，進而協助其管理人員處理此一問題。

本文以下各節整理如後：第 2 節說明 DNS 反射攻擊如何利用 DNS 伺服器來發動 DDoS 攻擊，第 3 節建議 DNS 伺服器管理者該如何保護其伺服器，以降低遭濫用的機會，第 4 節介紹在校園網路的環境下，我們所開發的自動偵測系統如何運用 NetFlow 流量資訊來加速偵測開放性 DNS 解析伺服器的 IP 位址，最後第 5 節為簡要的結論。

2. DNS 反射攻擊的運作原理

本節將介紹 DNS 反射攻擊是如何利用開放性 DNS 解析伺服器產生巨量網路流量攻擊受害者，從而了解如何避免遭利用。圖 3 為 DNS 反射攻擊之示意圖，攻擊者操控僵屍電腦(bot)對開放性 DNS 解析伺服器送出假造來源為受害者 IP 位址的 DNS 查詢(query)封包，因此這些提供服務的 DNS 伺服器自然將回應(response)封包送至受害者的 IP 位址。除了邀集夠多的 DNS 伺服器參與攻擊外，另一項能讓攻擊者事半功倍的因素就是 DNS 查詢與回應封包的放大因數(amplification factor)。以圖 4 的兩筆 DNS 查詢實例做說明，第一筆查詢與回應其 DNS 應用層訊息長度(不含 UDP 標頭)分別為 25 與 473 bytes，故其放大因數約為 19，第二筆查詢增加

DNSSEC 選項，則其查詢與回應分別為 36 與 1275 bytes，放大因數約為 35，可想而知攻擊者為促成低成本高效益的攻擊，會挑選能有較大放大因數的查詢組合，而開放性 DNS 解析伺服器正好符合讓其恣意查詢的需要(例如：在某處註冊長度很大 DNS 資源記錄，再刻意讓開放性 DNS 解析伺服器前去查詢)。再以第 2 筆查詢為例，若僅計算 DNS 回應訊息長度，對一部開放性 DNS 解析伺服器每秒進行 100 次查詢，就能產生 1.02 Mbps 的攻擊流量，而攻擊者的僵屍電腦僅付出 28.8 Kbps 頻寬，若邀集 1000 部 DNS 伺服器參與攻擊，就能產生 1 Gbps 攻擊流量(足以塞爆目前許多交換器或伺服器的網路界面)。根據 Open resolver project 2013/08/11 最新的統計，網際網路上具有威脅性的伺服器高達二千多萬部以上(會回應 udp/53 查詢的有 32,155,735 部，會正確回應 A 記錄的有 26,928,868 部)，對攻擊者而言，輕易就能找到夠多的幫手，累積夠多的網路流量來癱瘓受害者的網路，面對這類來自四面八方分散式的攻擊，受害者通常難以招架。

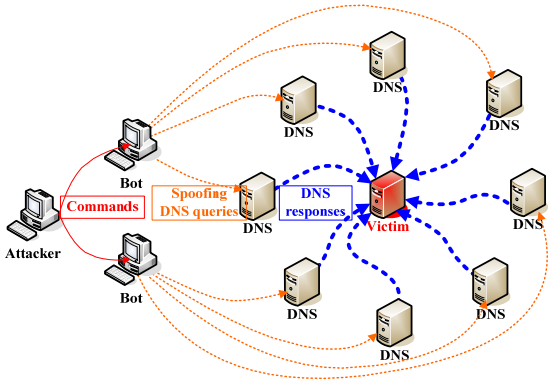


圖 3. DNS 反射攻擊示意圖

```
# dig +noignore @140.114.xx.76 isc.org any

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR
;; flags: qr tc rd ra; QUERY: 1, ANSWER: 11

;; QUESTION SECTION:
;isc.org.              IN     ANY

;; ANSWER SECTION:
isc.org.      34       IN     A        149.20.64.69
略…

;; Query time: 4 msec
;; MSG SIZE  rcvd: 47
```

```
# dig +noignore +dnssec @140.114.xx.76 isc.org any

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR
;; flags: qr rd ra; QUERY: 1, ANSWER: 16, ADDITIONAL:
3

;; QUESTION SECTION:
;isc.org.              IN     ANY

;; ANSWER SECTION:
isc.org.      24       IN     A        149.20.64.69
略…
isc.org.  7164         IN     DNSKEY   257 3 5 BEA 略…
;; Query time: 3 msec
;; MSG SIZE  rcvd: 1275
```

圖 4. 許可 DNS 遞迴查詢之回應

總之，DNS 反射攻擊對攻擊者而言具有匿跡、方便、難以防禦等優勢：

1. 使用假造來源 IP 位址的 UDP 封包，難以追溯出攻擊者與僵屍電腦的真實 IP 位址。此外，有些被利用的 DNS 伺服器管理者看到大量 DNS 查詢數，認為自己遭 DoS 攻擊，易誤判受害者為攻擊者，去檢舉反而增加受害者困擾。
2. 網路上數千萬部可資利用的開放性 DNS 解析伺服器存在，對攻擊者建立一支數量龐大的打手部隊不難。
3. 由於打手分散於世界各地，受害者難以用簡單的 IP 位址過濾來防禦，且通常受害者的出口網路會先被攻擊流量塞爆而束手無策。

因此，未來這類利用開放性 DNS 伺服器的攻擊將會層出不窮。

3. DNS 伺服器的保護作法

面對日益增多的攻擊，DNS 伺服器管理者可從限制服務對象與限制使用量兩方面來著手，以保護其設備，減少遭利用的機會。限制服務對象主要係根據用戶連線來源的 IP 位址，決定是否提供 DNS 查詢服務或遞迴查詢權限，藉此減少遭外面攻擊者濫用的機會，實務上可用防火牆或 DNS 應用軟體的 ACL (access control list)功能來限制。以防火牆直接阻斷非服務範圍內 IP 位址之 DNS 查詢封包的作法，處置較快也毋須產生回應封包，故不會被利用，且查詢者須等到連線逾時方知未能使用該服務(如圖 5)。而使用 ACL 拒絕服務的作法，查詢者可獲得回應訊息(REFUSED，如圖 6)，所幸回應訊息短，被攻擊者利用的價值不高（放大因數約為 1），不過仍會消耗 DNS 伺服器系統及少量網路資源。所以，對內部用戶提供遞迴查詢服務的遞迴名稱伺服器，使用防火牆直接阻斷非服務範圍的來源 IP 位址較為簡便；但對全世界開放查詢其管轄網域資料的授權名稱伺服器，無法限制來源 IP 位址，故須限制遞迴查詢功能，當查詢非所轄網域時回應訊息短(如圖 6)，可減低被利用的價值。早期 DNS 伺服器經常同時擔任遞迴名稱伺服器與授權名稱伺服器兩項工作，但在現今的網路環境下，基於安全及管理考量，應將兩者分開建置。

即使 DNS 伺服器已限制來源 IP 位址或拒絕遞迴查詢權限，仍難免遭到大量查詢而浪費系統資源，圖 7 為筆者觀察所維運校園 DNS 伺服器遭濫用的可能途徑，其中授權名稱伺服器雖已關閉遞

迴查詢權限，但有時攻擊者並不在意其低利用價值；而遞迴名稱伺服器可能因校內某些設定不當的開放性 DNS 伺服器轉送查詢(forwarder)，難免遭到校內用戶濫用。不論為何，大量查詢對伺服器即構成 DoS 攻擊，因此限制用戶查詢使用量(rate limit)有其必要性，作法上可用 IPS 設備或 DNS 應用軟體的功能，限制單一 IP 位址在單位時間內最大的查詢次數，藉此保護伺服器免於因某用戶不當使用而影響整體服務。目前我們使用 DNS response rate limiting [12]的軟體對 DNS 伺服器進行保護，圖 8 為限制使用量所進行的密集查詢測試結果，其中有一筆查詢不被回應，顯示限制已有作用，圖 9 為我們所管理的兩部校園 DNS 伺服器在同一時段內的查詢使用量曲線圖，其中圖 9(a)的伺服器未建置限制使用量保護，故有時因用戶濫用而造成查詢量激增至接近每秒 2000 次，而圖 9(b)的伺服器已建置限制使用量保護，則免於此異常情況。

```
# dig @140.114.xx.1 isc.org any

; <<>> DiG 9.6 <<>> @140.114.xx.1 isc.org a
;; global options: +cmd
;; connection timed out; no servers could be reached
```

圖 5 以防火牆阻斷查詢之結果

```
# dig +noignore @140.114.xx.10 isc.org any

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id:
36450
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;isc.org.                        IN      ANY

;; Query time: 2 msec
;; SERVER: 140.114.xx.10#53(140.114.xx.10)
;; WHEN: Wed Aug  7 10:33:31 2013
;; MSG SIZE  rcvd: 25
```

圖 6 以 ACL 拒絕查詢或不提供遞迴查詢之回應

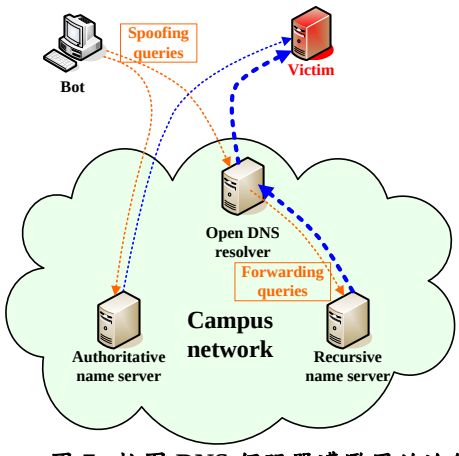
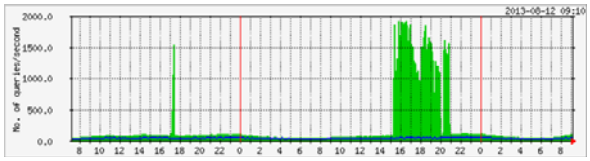


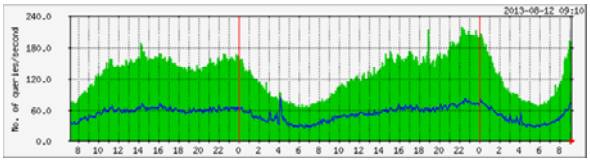
圖 7. 校園 DNS 伺服器遭濫用的途徑

```
# repeat 10 dig @140.114.xx.10 +noignore +short
+tries=1 +time=1 www.nthu.edu.tw a
140.114.69.135
140.114.69.135
140.114.69.135
140.114.69.135
140.114.69.135
;; connection timed out; no servers could be reached
140.114.69.135
140.114.69.135
140.114.69.135
```

圖 8. 限制使用量的密集查詢測試



(a) 未限制使用量



(b) 限制使用量

圖 9. 校園 DNS 伺服器之查詢量

4. 開放性 DNS 解析伺服器的偵測

要檢測校園網路內某 IP 位址是否為開放性 DNS 解析伺服器，最直接的方法就是由使用校外 IP 址的檢測器對檢測對象送出具有遞迴要求的 DNS 查詢封包，查詢非本校所轄網域的 DNS 資源記錄，再視其回應結果判定，若回應狀態為 NoError 且其 Answer 數目非零(如圖 4)，則為開放性 DNS 解析伺服器，其餘狀況則為非。試想若對全校數萬個 IP 位址逐一檢測，每一 IP 位址以 10 秒計，所耗費時間將超過一天以上，況且檢測時受檢電腦未必開機中，故漏判情況勢必更多。為解決檢測數目過多與停機漏判的問題，我們利用校園連外網路骨幹路由器的即時 NetFlow 資訊，發展「開放性 DNS 解析伺服器偵測系統」，其系統架構如圖 10 所示。先將 NetFlow 資料進行簡單分析，篩選目的 IP 位址屬校外，來源 IP 位址屬校內，且來源通訊埠為 udp/53 的流量記錄(如圖 11)，則這些校內 IP 位址為 DNS 伺服器的可能名單，再即時將它送交建置於校外的檢測系統進行確認是否為開放性 DNS 解析伺服器。此外，為避免不必要的連續檢測，故設定同一 IP 位址在某時間內(暫設一天)僅檢測一次。

表 1 為本系統由 2013/08/06 至 08/12 運作一週的結果統計，每天平均有 12,782 個校內 IP 位址曾經上網使用(由骨幹路由器上計得，時值暑假期間較開學期間少)，日平均檢測數 284 個 IP 位址，僅佔上網使用 IP 位址數的 2.2%，已大幅降低檢測的工作量，日平均確認率約為 45.8%(確認數/檢測數)，顯示在疑似 DNS 伺服器中有相當高比率具有開放

性 DNS 解析伺服器問題。累計一週確認為開放性 DNS 解析伺服器(排除重覆 IP 位址)共計 248 個，進一步嘗試查詢其軟體版本(用 dig @server_ip version.bind ch txt)，統計結果如圖 12，共有 153 筆回應，其中 dnsmasq 佔 126 筆，多數 IP 位址在同一網段，經訪查該單位網管人員表示係無線網路服務使用，有些為無線路由器、寬頻防火牆路由器，因此，除了電腦外，像這類網路設備亦可能具有開放性 DNS 解析伺服器問題須注意及處理。由上述結果顯示，本偵測系統可以即時有效地偵測出校園網路內之開放性 DNS 解析伺服器，但若要更進一步即時解決這些伺服器被利用的問題，未來可納入本校「校園網路安全事故自動防治系統」[13]，一旦發現便阻斷其 IP 封包並公告，即可達到即時防治的效果。不過，由於現在多數電腦使用者對開放性 DNS 解析伺服器這個問題仍不熟悉，且校園內仍有部分授權名稱伺服器具有此問題，故暫不宜冒然進行阻斷以免中斷某些單位的 DNS 服務，現階段仍以宣導並通知各單位改善，待時機成熟後，再納入自動防治系統較為適當。

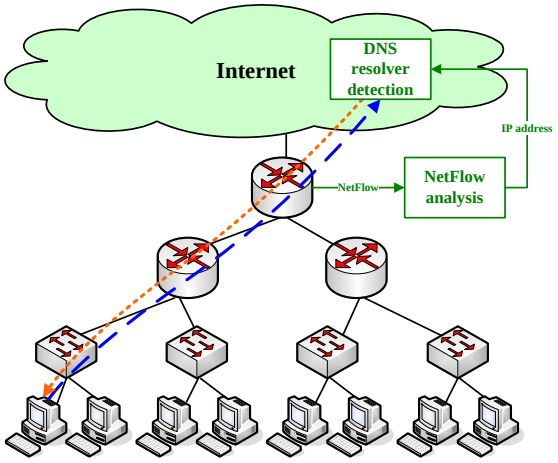


圖 10. 開放性 DNS 解析器偵測系統架構

SrcIPaddress	SrcP	DstIPaddress	P	Pkts
140.114.xx.10	53	210.xx.xxx.102	17	21672
140.114.xx.1	53	69.xx.xx.12	17	1997
140.114.xx.59	53	90.xx.xx.70	17	1
140.114.xx.59	53	109.xxx.xxx.98	17	1
140.114.xx.59	53	178.xxx.xxx.112	17	13
140.114.xx.136	53	61.xxx.x.195	17	1
140.114.xx.159	53	178.xx.xxx.16	17	138

圖 11. 疑似 DNS 伺服器的校內 IP 位址

表 1. 開放性 DNS 解析器一週偵測結果統計

日期	使用 IP 數	檢測數	確認數
08/06 Tue.	13,751	358 (2.6%)	171 (47.8%)
08/07 Wed.	13,814	277 (2.0%)	120 (43.3%)
08/08 Thu.	13,612	336 (2.5%)	173 (51.5%)
08/09 Fri.	13,152	332 (2.5%)	161 (48.5%)
08/10 Sat.	10,557	194 (1.8%)	81 (41.8%)
08/11 Sun.	10,768	268 (2.5%)	129 (48.1%)
08/12 Mon.	13,823	221 (1.6%)	88 (39.8%)
平均	12,782	284 (2.2%)	132 (45.8%)

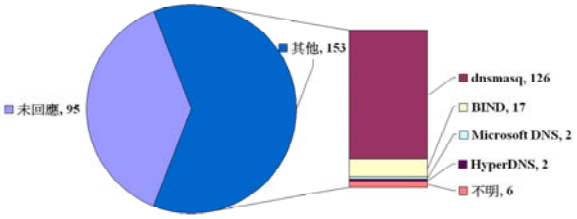


圖 12. 開放性 DNS 解析器軟體統計

5. 結論

本文已探討開放性 DNS 解析伺服器被利用做為 DDoS 攻擊打手的問題將日益嚴重，究其原因常來自於電腦管理者對軟體安裝或設定不慎所致，尤其並非人人都熟悉 DNS 伺服器的管理，故常在不知情的情況下發生此一問題，即使想自行驗證內部網路的伺服器是否具開放性，尚須有外部網路的配合，仍諸多不便，因此，本文除了提供 DNS 伺服器保護的建議作法外，並已實作「開放性 DNS 解析伺服器偵測系統」，以協助各單位網管人員找出內部的開放性 DNS 解析伺服器，進而修補問題。偵測結果顯示本系統能即時有效地找出校園網路內的開放性 DNS 解析伺服器，未來將結合「校園網路安全事故自動防治系統」，更可達到即時防治的效果。

參考文獻

[1] Domain name system, http://en.wikipedia.org/wiki/Domain_Name_System

[2] R. Vaughn and G. Evron, “DNS amplification attacks, preliminary release,” 2006.

[3] J. Markoff and N. Perlroth, “Firm is accused of sending spam, and fight jams Internet,” http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html, 2013.

[4] M. Prince, “The DDoS that knocked Spamhaus offline,” http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho.

[5] P. Mockapetris, “Domain names – concepts and facilties,” RFC 1034, 1987.

[6] P. Mockapetris, “Domain names – implementation and specification,” RFC 1035, 1987.

[7] The measurement factory, “DNS SURVEY: OPEN RESOLVERS,” http://dns.measurement-factory.com/surveys/openresolvers.html

[8] DNS spoofing (or DNS cache poisoning), http://en.wikipedia.org/wiki/DNS_spoofing

[9] Open Resolver Project, http://openresolverproject.org/.

[10] 賴守全、謝木政、藍松月，“開放性郵件中繼主機防治系統之設計與實作，” TANet 2003.

[11] NetFlow, http://en.wikipedia.org/wiki/NetFlow

[12] Response Rate Limiting in the Domain Name System (DNS RRL), http://www.redbarn.org/dns/ratelimits.

[13] 賴守全，謝木政，“校園網路安全事故自動防治系統之設計與實作，” TANet 2002.