即時偵測防治 Internet Worm

陳嘉玫、黃世昆、陳年興、鍾明勳
台灣電腦網路危機處理中心
http://www.cert.org.tw

摘要

台灣學術網路於 2001 年 8 月份遭嚴重病毒攻擊，各區網中心所受波及影響很大。近年來，網路攻擊行為與 Internet Worm 造成嚴重的網路威脅，解決網路攻擊並提出一套有效即時預警系統是迫切而且必要的。本文我們試著以網路流量的監測工具 NetFlow，提出一套即時而有效的偵測此類攻擊的方法，並且在這次 Code Red、Nimda 攻擊發起時有效的將中山大學網路的損害減至最低。

關鍵詞：NetFlow, Internet Worm, Virus, DoS

前言

2001年八月份的Code Red Worm和九月份的 Nimda Worm 造成台灣學術網路各區網中心嚴重的影響[1]，但因這種型式的Worm對使用者本身傷害不大，往往使用者被感染仍不自覺，但是對路由器、防火牆、代理伺服器、郵件伺服器等網路重要設備損害很大，利用大量的封包影響網路基本運作。

近年來研究如何在網路上即時的找出入侵及攻擊的相關研究越來越被重視，本文試圖利用NetFlow網路流量資料分析出感染worm的主機的網路流量Pattern，並以此為判斷依據找出可能的感染主機，以通知網路管理者做出適切的處理並通知使用者掃毒，恢復網路正常運做。由於中山大學是台灣學術網路南部區網中心，高雄縣市、屏東縣市及台東、澎湖等網路皆經由中山大學與 TANet 的相連接，為維護正常之教學與研究網路傳輸品質，網路安全防護更是刻不容緩。希望藉此研究技術在2001年8月份 Code Red 及9月 Nimda 攻擊發作時適當的保護中山大學網路的正常運作，並提供中山大學計算機與網路中心校內感染主機名單，做有效的防制。

1. NetFlow 簡介

NetFlow[2]是 Cisco 發展的流量統計協定，這些統計被有效的使用在網路管理、計數及網路規劃等，目前廣受各家廠商支援。Flow 指的是特定來源和目地的單向流量資料，也就是來源 IP、目地 IP、來源 Port、目地 Port 四個屬性相同的封包之資料傳送量總和為一個 Flow。

NetFlow 架構

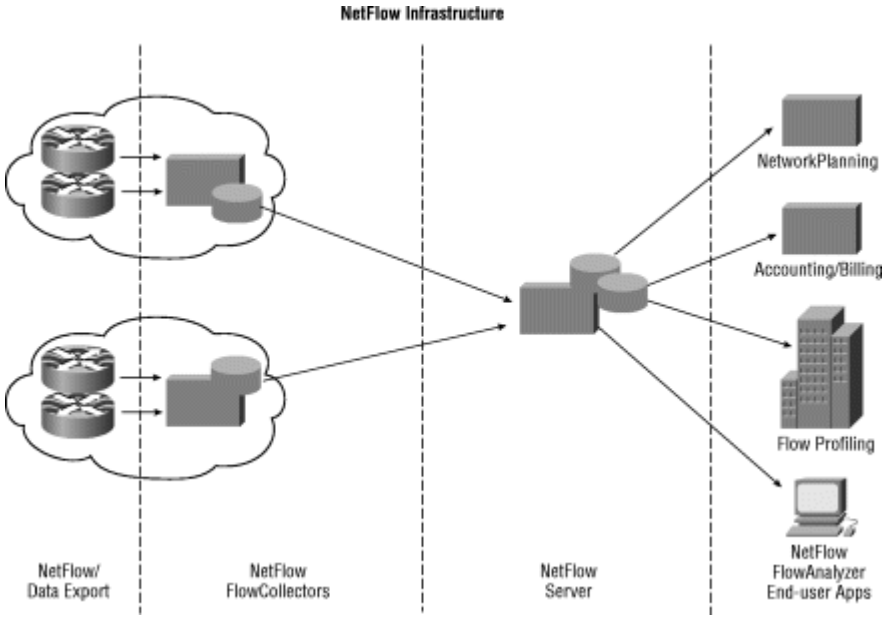

圖 1. NetFlow 架構

NetFlow 架構共可分為四部分，如圖 1.所示。NetFlow Data Export 支援 NetFlow 的設備，如 Router、Sniffer。NetFlow。Net Flow FlowCollector 提供快速、準確與便利的資料收集方式，接收 UDP 協定的 NetFlow 封包，存進 NetFlow Server。NetFlow Server 可同時由多個 FlowCollectors 收集 datafiles，但無法每次由單一 FlowCollector 取得一個以上的 datafile，以避免不當的執行影響 NetFlow FlowCollector，並降低磁碟與 CPU 的負荷。NetFlow FlowAnyalyzer 是網路傳輸分析工具，利用 NetFlow Server 中的資料做統計分析，如各別 IP 傳輸量、協定分佈、封包大小分佈、異常偵測[8]。

NetFlow 可提供下列資訊，分析網路異常狀況：

種類	功能／內容
來源 IP、目地 IP、來源 port、目地 port	主機、服務傳輸量

協定種類	TCP、UDP、ICMP 等等
入口介面、出口介面	流量在實體層的來源和目地，因 IP 層可以偽造。
TCP Flag	■ 可以判斷連線的性質，開始(SYN)、過程(SYN+ACK)、結束(FIN) ■ 可以判斷攻擊的性質，如 SYN Flood、ACK Flood、OOB Attack
ICMP Type	■ 可以判斷網路異常，Destination Unreachable ■ 可以判斷網路攻擊，ICMP Redirect
packet 數目、byte 數目、開始時間、結束時間	Workload 分析，例如：攻擊行為通常封包小數量多，傳輸 MP3 的 Flow 主要在 4-6 MB
ASN(Autonomous System Number)	在與多個 ISP 互連時可直接統計互連流量，不需依照 IP 判斷 ISP

2. 即時偵測與防治

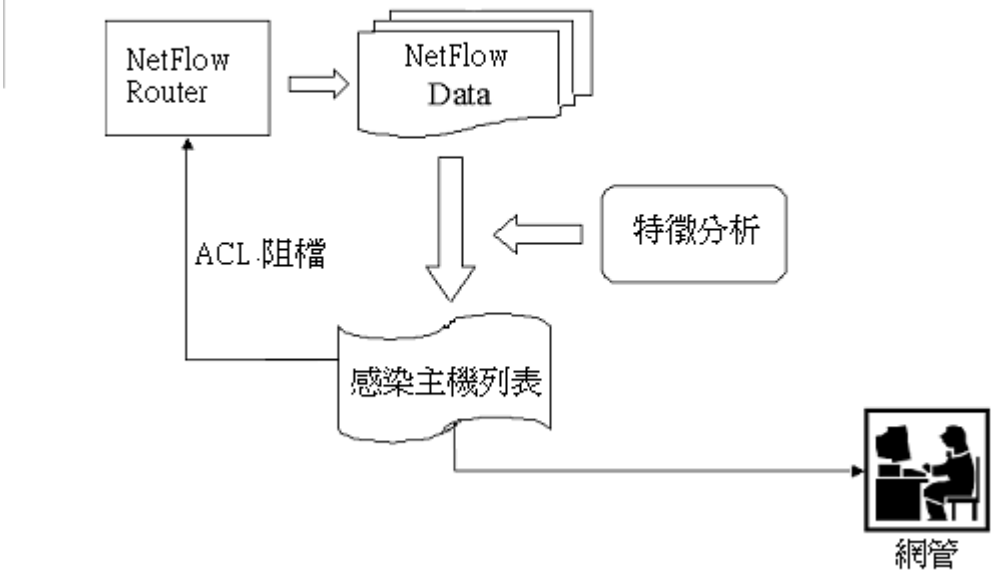

圖 2. NetFlow 偵測流程

圖 2. 簡述 NetFlow 的偵測流程。利用已知的 Worm 特徵，每五分鐘分析一次 NetFlow 資料，找出受感染的主機，並通知網管人員處理，在 Router 設定 Access Control List 做適當的隔離。

3. Internet Worm

Worm 是利用主機的安全弱點進行自動化入侵與繁衍的惡意程式碼。利用的弱點包括作業系統的弱點、應用程式的弱點、不安全的權限設定、伺服器的弱點、人類不安全的使用習慣。

3.1 Code Red 簡介

Code Red 是一隻會自我繁殖入侵系統的惡意程式碼，利用微軟 IIS Web Server 的安全性漏洞入侵，並在受害者主機上自我繁殖，入侵後留下後門，同時產生 600 個執行緒，隨機產生 IP 嘗試入侵沒有安裝修補程式的 IIS WEB 伺服器，被植入 Code Red 的主機可能同時多次掃瞄同一台主機，沒有受到感染的主機可能會成為 Code Red 的攻擊目標，受到 DOS(denial of service)的攻擊。由於持續變換目地 IP 位置，消耗路由器資源，導致低階路由器當機，中高階路由器效能下降。自七月中旬以來，由於 Code Red 嚴重肆虐，不論是個人用戶、企業組織與學術單位皆受到其嚴重戕害。

微軟公司在 6/20 發佈修正檔，7/19 全球已經有 250,000 部主機感染，然而台灣大部份主機仍然沒有修正；直到八月初災情擴大，低階路由器支撐不住，導致網路中斷，才有大規模的修正行動，顯見使用者多半輕忽系統漏洞的警訊及網路保全的重要性。除了妥善維護重要資料的備份與維護，定期的防毒防災安檢更是不可或缺的重要工作。

3.2 Nimda 簡介

Nimda (別名 W32/Nimda.A@mm, I-Worm.Nimda, Readme,Readme.exe 等)會利用現有網站提供受感染檔案下載，並利用 end user 的主機掃描其他有漏洞的網站，這使得 Nimda 可輕易地入侵受防火牆屏障的 intranet，強大的破壞力透過網際網路在全球迅速傳播，破壞力不遜於 Code Red。

Nimda 混合使用多種傳播方式：

1. 和 Code Red 一樣使用 IIS 之漏洞
2. 被攻擊主機之前遭 Code Red worm 或 sadmid/IIS worm 感染留下之後
3. IE 以及 Outlook Express 自動開啟檔案的漏洞
4. 修改 Web Server 之網頁使得拜訪者自動下載 Nimda
5. 上傳至網路芳鄰可任意讀寫之資料夾
6. E-Mail

Nimda 結合上述多種常見的攻擊模式，是其迅速擴張肆虐的主因，一天之內全球都受到感染，Nimda 會針對系統漏洞進行複製與散播，將 C 磁碟機設為資源共享，任意複製、修改、刪除重要檔案文件、破壞受感染的系統，並加重網路承載。另外因為使用網路芳鄰，因此除了路由器效能受影響外，LAN 的效能也受影響。如果受到感染後沒有徹底清除並修補系統漏洞，將會對網路安全造成重大危害。

3.3 一般性的流量特徵

因 worm 的特性將造成異常流量，因此，應先找出正常與異常流量之特徵，才可比較分析何處發生 worm 的感染。依照 worm 所利用的安全弱點型式，有直接和間接的流量特徵。

直接流量特徵為攻擊者對受害者的直接連線，利用作業系統漏洞(例：Remote Procedure Call)、不安全的權限設定(例：網路芳鄰開放任意讀寫)、伺服器的漏洞(例：透過 Web Server 入侵)。已被感染的主機會產生大量對外攻擊的連線，因此可以先找出封包數量或 flow 數量異常之主機，再分析相關之資料。

間接流量特徵以 email worm 為代表，利用的是應用程式弱點(例：mail client 自動開啟附加檔案並執行)、不安全使用習慣(例：使用者開啟來源不名的郵件附加檔案)，表現在流量上為 email 相關的流量異常增加。

3.4 正常流量與異常流量比較

圖 3. 是 5/20 及 9/20 某一時間的流量分析，5/20 是一般正常流量，統計資料顯示，9/20 宿網對校網 WWW 的 flow 數異常增加，表示宿網機器遭受 Code Red 網蟲攻擊。更進一步地，希望能查出哪些主機受到感染，以下 IP 之資料為假 IP。圖 4. 顯示一般正常 www 流量資料，而圖 5. 顯示 9/10 某一時刻大量 www 連線遠超過正常 www 流量的前四名，因此判斷他們感染 worm。

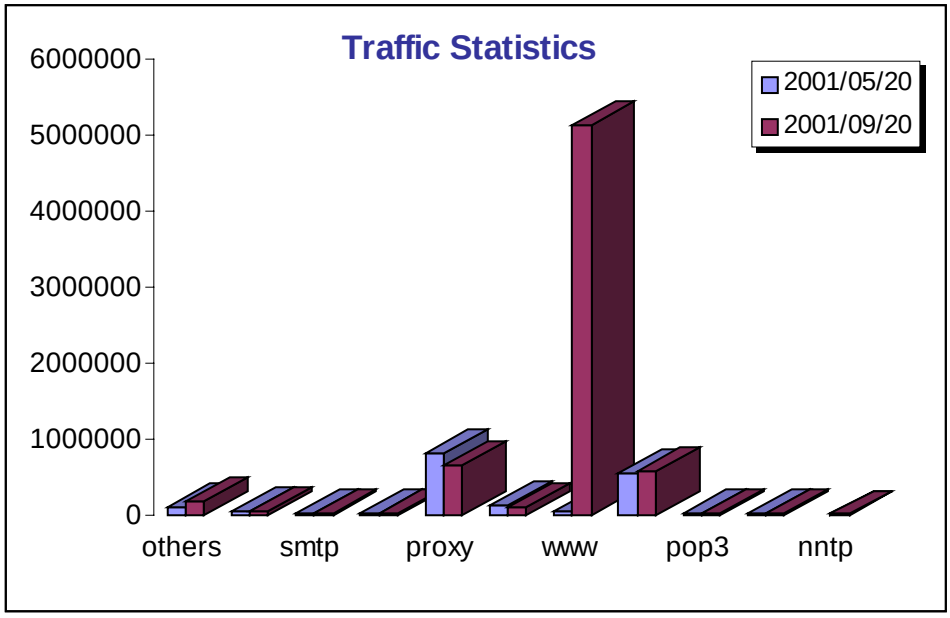

圖 3. 流量分析

正常

2001-06-10 Statistics of www Traffic

Source	Flows	%	KPackets	%	MBytes	%
Dorm ==> NSYSU	78785	4.232%	1211.053	0.589%	168.041	0.104%
10.1.4.147	722	0.916%	83.303	6.879%	7.202	4.286%
10.1.8.35	8109	10.293%	40.671	3.358%	5.618	3.344%
10.1.8.174	2	0.003%	3.440	0.284%	4.714	2.805%
10.1.8.148	601	0.763%	18.671	1.542%	4.356	2.592%
10.1.82.114	765	0.971%	28.982	2.393%	3.221	1.917%
10.1.7.66	819	1.040%	10.206	0.843%	2.418	1.439%
10.1.3.219	247	0.314%	3.674	0.303%	1.975	1.175%
10.1.11.157	59	0.075%	23.712	1.958%	1.959	1.166%
10.1.12.72	100	0.127%	23.240	1.919%	1.946	1.158%
10.1.5.72	418	0.531%	19.693	1.626%	1.931	1.149%

圖 4. 2001/06/10 Statistics of www Traffic

異常

2001-09-10 Statistics of www Traffic

Source	Flows	%	KPackets	%	MBytes	%
Dorm ==> NSYSU	1512195	59.971%	4836.612	0.992%	493.938	0.255%
10.1.10.121	**904749**	59.830%	2738.732	56.625%	243.144	49.226%
10.1.9.56	**183510**	12.135%	641.466	13.263%	55.712	11.279%
10.1.9.64	**192345**	12.720%	581.560	12.024%	51.249	10.376%
10.1.12.186	**145398**	9.615%	439.312	9.083%	38.929	7.881%
10.1.10.85	266	0.018%	21.632	0.447%	28.179	5.705%
10.1.15.5	335	0.022%	6.592	0.136%	6.641	1.345%
10.1.8.171	1864	0.123%	6.321	0.131%	4.719	0.955%
10.1.82.235	14455	0.956%	43.852	0.907%	3.835	0.776%
10.1.6.151	24	0.002%	3.112	0.064%	3.721	0.753%
10.1.81.8	224	0.015%	3.645	0.075%	3.421	0.693%

圖 5. 2001-09-10 Statistics of www Traffic

3.5 Nimda Worm 特徵

Nimda 由於使用多種漏洞，並且依照被攻擊主機有不同行為， 無法以特定 Packet 數量和 Byte 數量作為判斷條件，因此採用 DstPort = 80 且五分鐘內同一 IP 之 flow 數大於 threshhold 判斷。

由於 CodeRed II 和 Nimda 的設計是 50%的機率攻擊同一 Class B IP，25%之機率攻擊同一 Class A IP， 25%的機率攻擊其它 IP， 因此在上游之 router 記錄到之 flow 數量會較少。若遭受感染，則其所屬之終端 router 的 flow 數量會異於正常。我們的 threshold 設定為：在終端 router， 內部感染的主機每五分鐘約有 1000 個以上之 flow，最高有五分鐘內超過 30000 個 flow。

4. 結論

利用 NetFlow 可以即時有效的找出感染 Worm 的主機，避免災情擴大，建議擁有 NetFlow Router 的單位建制監測系統，在未來將類似攻擊的傷害降到最低。CodeRed 和 Nimda 所利用的緩衝區溢位問題屢見不鮮，顯見系統軟體設計有疏

漏之虞，加上人為的資訊衛生習慣不良，導致網蟲迅速擴張蔓延。除了安全偵防工具的利用外，在系統建構、管理與維護上落實嚴謹的資訊安全政策更可提升自我防護能力。

此外，使用者行為也關係個整體網路之安全性。我們有以下幾點建議，期望減少網蟲之傷害：

1. 個人電腦及伺服器應安裝防毒軟體，定期或不定期進行偵測、掃毒，並隨時更新病毒碼及掃描引擎，以防止病毒入侵。
2. 謹慎使用可掃除電腦病毒及系統回復軟體；使用前應充分了解電腦病毒特性，以及確定解毒軟體的功效。
3. 若遭病毒感染後，應立即追蹤病源並掌握擴散狀況，且徹底進行消毒。
4. 不任意進入主題或意圖不明的電腦網站。
5. 傳送電子郵件前應先檢查本身是否含有病毒，收件後亦應先檢查確定後再開啟。
6. 安裝網路防毒系統，以攔截、防制病毒進入區域網路，使電腦病毒無法侵入單位內部。
7. 檔案伺服器（FTP）上傳及下載之檔案應先進行掃毒。
8. 做好系統備援環境並定期備份資料，以防系統遭破壞時能配合災變應變程序即時恢復運作，例如資料碟備份或 Ghost。
9. 不開啟來路不明的電子郵件，不安裝、不執行來路不明的軟體。
10. 關閉不必要的網路服務。
11. 隨時注意電腦網路安全相關議題，定期檢視系統記錄檔、安裝最新修補程式，並建立網路保全重大事件聯絡之管道。

5. 參考文獻

[1] http://www.edu.tw:81/tanet/bulletin/board1.html
http://groups.google.com/groups?hl=zh-TW&frame=right&th=d00a208f96d9bee3&seekm=3hjBVd%24AuU%40bbs.ntit.edu.tw#s

[2] White Paper: NetFlow Services and Applications
http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm

[3] Cflowd
http://www.caida.org/tools/measurement/cflowd/

[4] CAIDA Worklad Characterization
http://www.caida.org/analysis/workload/

[5] CodeRed
http://www.cert.org/advisories/CA-2001-19.html
http://www.eeye.com/html/Research/Advisories/AL20010717.html

[6] Nimda Worm
http://www.cert.org/advisories/CA-2001-26.html
http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.e@mm.html

[7] Flow-tools
http://www.net.ohio-state.edu/software/

[8] 楊子翔、蔡錫鈞， Network DoS/DDoS 攻擊及預防方法之研究，TANet 2000 研討會
http://www.ncku.edu.tw/TANET2000/download/paper/A3-2tanetI06.doc