個案分析-

C 大學的 C&C 分析報告

TACERT 臺灣學術網路危機處理中心團隊製

2012/3

目錄

概要

■ 主機資訊

所在地及所屬單位：C 大學資工系，提供學生實驗之主機

網路位址：192.168.103.148（IP 已經過處理）

作業系統：ubuntu 10

開啟 port 及運行服務：

- Port : 22 (ssh)
- Port : 80 (nignx http proxy)

■ 事件經過

2012/2/24	技服中心發現異常，許多 Zbot 連向 192.168.103.148，隨即請 C 大學 mirror 192.168.103.148 主機封包
2012/3/01	到 C 大學取資料，因封包數量太多，mirror 封包的主機早就不堪負荷。當天技服立即架設另外一組硬體 mirror 封包，且只過濾出 tcp 的
2012/3/07	取網路 pcap 檔案以及主機資料

■ 入侵原因

使用者開放 root 帳號遠端登入，並且設定過於簡單的密碼：123

■ 惡意行為

Zbot 中繼站：192.168.103.148 上有由 Nignx 套件所架設的 Http proxy，提供 Zbot 與 C&C 間封包的 relay，192.168.103.148 收到 Http request 之後，會將流量 relay 給位於荷蘭的 85.17.138.133。

特定埠號掃描:除了扮演 relay 流量的中繼站，192.168.103.148 也對許多 Class B 網域進行 5900 port 的掃描，5900 port 主要運行 vnc 服務。

■ 分析資料如下列：

192.168.103.148 本機端的網路封包，僅有 tcp 部份，分為兩大類：

- Nginx Http Proxy 接收與轉送的流量
- 5900 port Scan

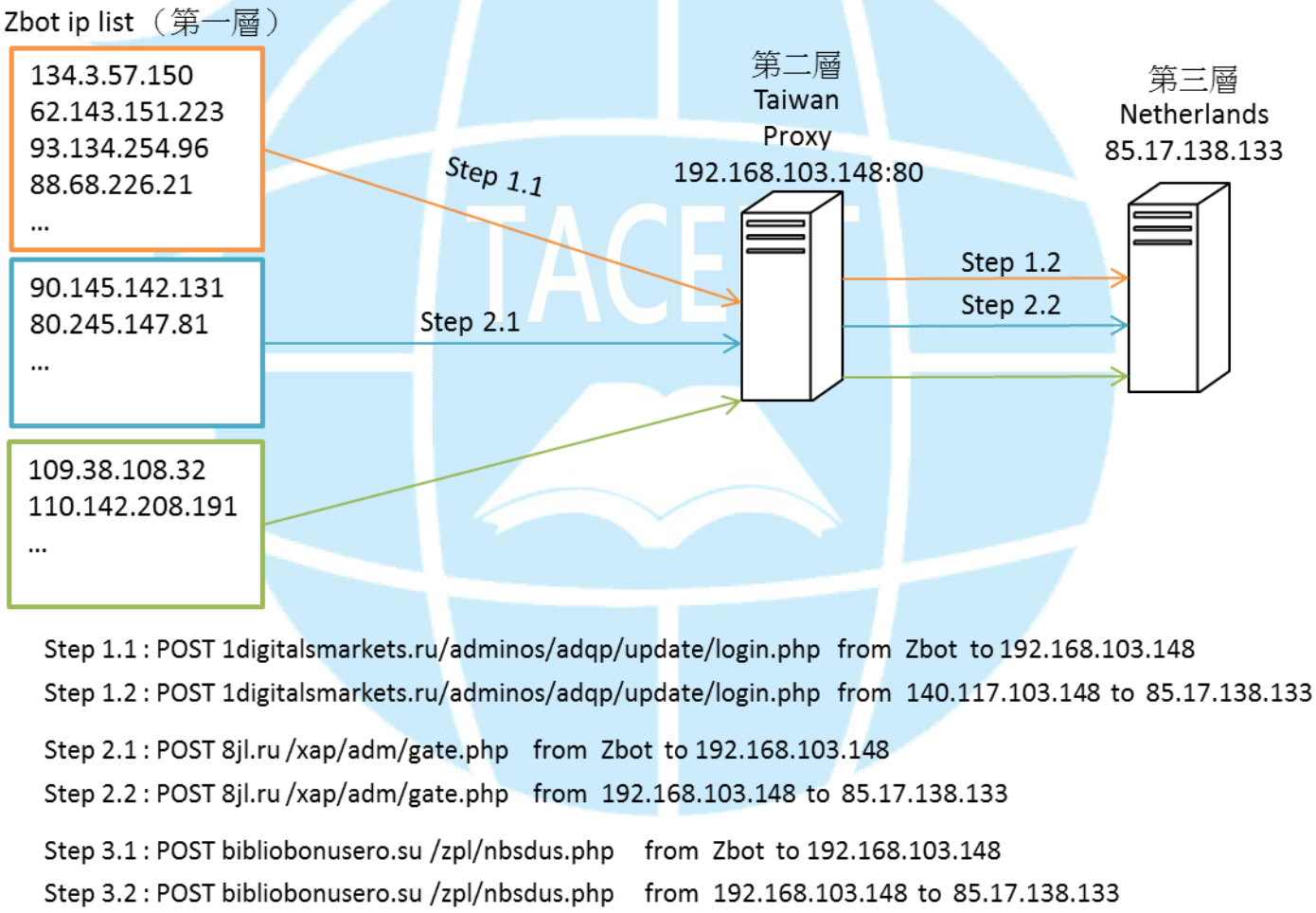
192.168.103.148 本機端特定資料夾以及有關 192.168.103.148 主機的資訊

- /var/log ：空
- /home/main ：僅有學生實驗資料
- /root ：駭客掃描工具
- /root/.history ：空
- /etc/passwd ：新增的帳號只有 main，由學生安裝時所增加
- /usr/local/nginx ：僅有 nginx 設定檔

Zbot 中繼站分析

在 192.168.103.148 本機端 pcap 檔，至少可以看到三層的架構，如圖一所示，192.168.103.148 扮演中繼站（第二層），relay 第一層 Zbot 的流量給第三層的 85.17.138.133，192.168.103.148 本身沒有任何 web 資料。

這樣的架構使得底層的 Zbot 不會有最上層主機的 IP，即使下層的 Zbot 被抓到了，也只會得到連線的 URL，URL 對應的 IP 全部都指向第二層的 proxy。Zbot IP List 由於數量眾多，圖一中僅列出部份。每一個 Zbot IP 所連線的 Domain 以及 URI 都是固定的，Domain 由拿到的 PCAP 檔分析，列出如表一。Domain 所對應的第二層 proxy 有數台，C 大學的只是其一。



圖一、relay 資料架構圖

表一、與 192.168.103.148 對應的 Domain

1	1digitalsmarkets.ru
2	8jl.ru

3	9iy.ru
4	axiomhotel.com
5	bibliobonusero.su
6	brainrace.ru
7	clayspheregan.com
8	closerchillaut.su
9	cutenews.net
10	diegosancheze.com
11	ecrxlibgchux.eu
12	emivohngu.ru
13	f53fsa1245.in
14	fudtem.eu
15	g.forsal.pl
16	gitasmarkets.ru
17	hightqwalutize.su
18	holiwarikloda.ru
19	hubooyeew.ru
20	indyware.ru
21	izmeritelshop.ru
22	jfdiopv.eu
23	jokerthelrerkomitunglat.ru
24	keyboardbuckse.su
25	maskclub.com
26	modnie-pricheski.ru
27	movescatchats.com
28	neonlioncarfia.su
29	oldairbase.com
30	oposumschoone.com
31	plasticinetec.ru
32	qdqmnmwbykid.eu
33	rjrpexaicsdt.eu
34	secretsvodrah.com
35	slimclock.com
36	spidermanshop.ru
37	tablepack.ru
38	taskdream.com
39	telecurveopora.com
40	tiger-g2.com
41	tripslokabucks.su
42	undircilerdez.com

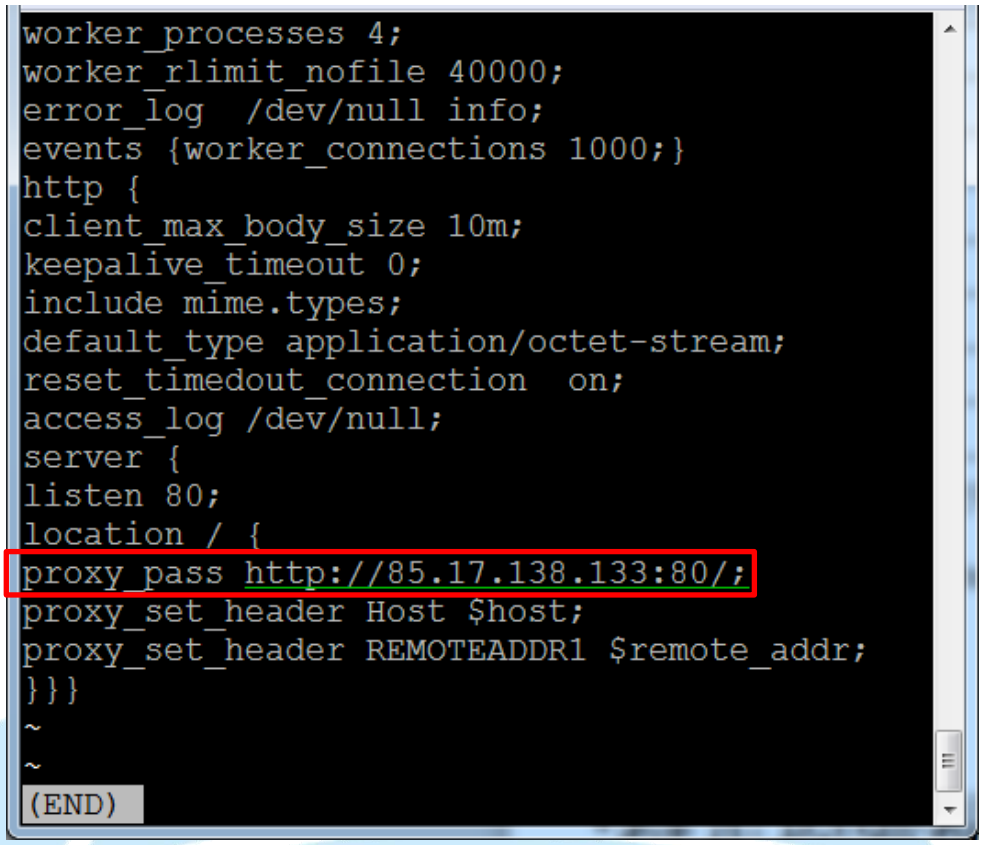
43	virtegelinosea.su
44	vlosgenawsyy.eu
45	wallstreet-fucked.com
46	wardeed.ru
47	wertubublersco.su
48	wrapweb.ru

表一的 Doamin 使用 fastflux 技術，除了對應到 192.168.103.148，也與表二的其他 IP（3/1 至 3/7 間查詢）輪流對應。

1	124.133.228.122	中國
2	192.168.103.148	台灣
3	208.115.203.138	阿爾巴尼亞
4	208.91.197.54	Virgin Islands (British)
5	209.141.60.202	加拿大
6	217.24.246.7	義大利
7	218.12.4.254	中國
8	221.194.146.109	中國
9	60.19.30.135	中國

表二、與 192.168.103.148 同層的 proxy

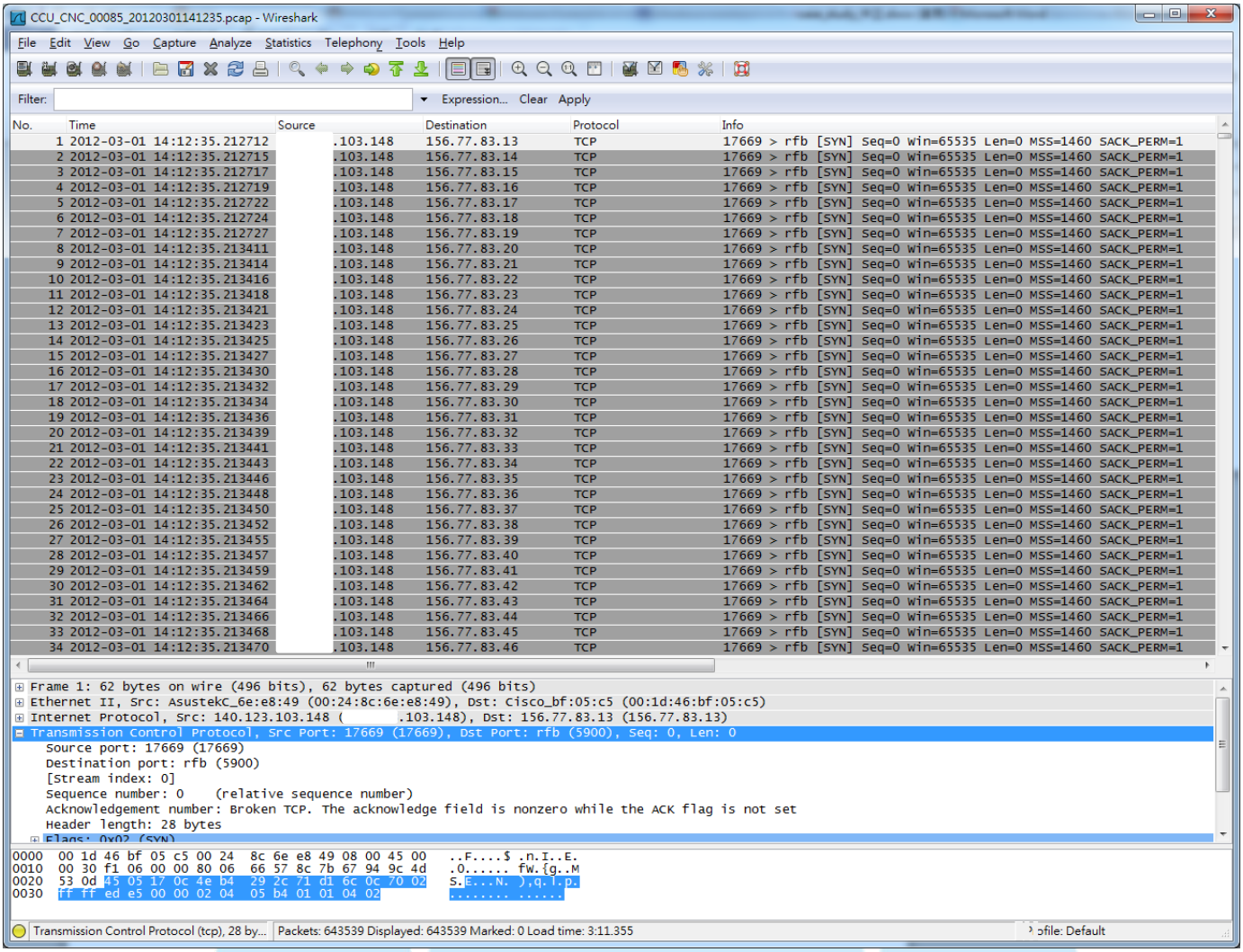
192.168.103.148 使用 Nginx 這個套件提供 Http Proxy 服務，在 Nginx 設定檔裡面，所有的紀錄檔都已經導向/dev/null，沒有留下任何紀錄檔，僅有 Nginx 設定檔。



圖二、192.168.103.148 主機的 nginx.conf 將主機設定為 proxy，流量都 relay 到 85.17.138.133

特定埠號掃描

192.168.103.148 在 relay 資料時，也同時大規模掃描多個 Class B 網段的 5900 埠，圖三僅列出某部份。在主機裡，也發現/root 下面有掃描的小程式。掃描程式列表如圖四，圖五則是 pass_file 的部份內容，裡面存放了掃描用的弱帳號密碼組合。



圖三、192.168.103.148 大規模掃描 5900 埠的封包

```
34:~/doiaruscan# ll
total 1408
---x--x--x 1 root root      0 2006-02-20 12:32 193.148.pscan.22
---x--x--x 1 root root      0 2006-02-22 12:16 200.118.pscan.22
---x--x--x 1 root root  18948 2006-01-01 13:31 213.246.pscan.22
---x--x--x 1 root root    265 2004-11-24 16:21 gen-pass.sh
---x--x--x 1 root root     89 2005-04-18 12:29 go.sh
-rw-r--r-- 1 root root  12947 2012-03-18 22:54 mfu.txt
---x--x--x 1 root root  53792 2006-02-14 08:28 pass_file
---x--x--x 1 root root  21407 2004-07-21 14:58 pscan2
---x--x--x 1 root root 453972 2004-07-12 11:09 ss
---x--x--x 1 root root 842736 2004-11-24 05:34 ssh-scan
---x--x--x 1 root root    546 2006-01-15 05:46 start
---x--x--x 1 root root      0 2006-02-14 09:25 vuln.txt
```

圖四、置於/root 下的掃描小程式

```
34:~/doiaruscan# head -20 pass_file
webmaster webmaster
root root
ftp ftp
sales sales
admin admin
andrea andrea
backup backup
guest guest
guest1 guest1
guest2 guest2
guest3 guest3
guest4 guest4
guest5 guest5
guest6 guest6
guest7 guest7
guest8 guest8
guest9 guest9
guest10 guest10
michael michael
gigi gigi
```

圖五、pass_file 部份內容

主機其他資料分析

/var/log 下存放許多紀錄檔，包括使用者登入登出紀錄，在這個部份，和 NGINX 服務的紀錄檔一樣，都已經導向/dev/null，入侵者在紀錄上的抹除上面十分徹底，沒有留下任何「登入」資訊。

lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 auth.log -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 btmp.1 -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 lastlog -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 messages -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 secure -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 security -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 utx.lastlogin -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 utx.log -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 wtmp.1 -> /dev/null
lrwxrwxrwx 1 root	root	9 2012-03-14 22:47 xferlog -> /dev/null

建議措施

- 各種遠端連線（SSH、VPN、VNC 等）的帳號密碼建議定時更新
- 最大權限管理者建議限制遠端登入位址
- 密碼建議使用英數與特殊符號夾雜
- 不與其他人分享密碼

調查[1]指出，密碼一直都是資安裡面最弱的一環，有七成以上的網路服務（各種遠端登入、網路銀行等等）僅使用密碼保護，十個人裡面有四個人至少與一個人共用密碼，許多人使用同一組密碼登入各種不同的網路服務，有一半以上的使用者從來不使用特殊字元作為密碼，十個裡面有兩個使用自己的生日或是重要紀念日當密碼（僅有數字），而此事件的入侵手法也是因為主機設定讓 root 可以遠端登入，並且使用弱密碼 123，讓駭客輕而易舉取得主機使用權限。

參考

[1] Surprise! Passwords Are (Still) Weak Link in Security Chain
http://www.pcworld.com/businesscenter/article/207718/surprise_passwords_are_still_weak_link_in_security_chain.html